Modelling and Simulation Applications on Cyber-Physical Systems' Security and Resilience

By

KONSTANTINOS MARASLIS

Department of Civil Engineering
UNIVERSITY OF BRISTOL

A dissertation submitted to the University of Bristol in accordance with the requirements of the degree of DOCTOR OF PHILOSOPHY in the Faculty of Engineering.

FEBRUARY 28, 2019

ABSTRACT

As our needs are constantly advancing, the Cyber-Physical Systems (CPS) that cover these needs should be able to handle more and more complexity. No matter which of the many available definitions of System one may accept, two things are certain; they are ubiquitous and keeping them safe and resilient is, by any measure, extremely important and difficult at the same time. Many causes are responsible for this difficulty, the most significant of which being the redundancy of some systems' components, their use within a context different to that they were designed for and finally the fact that their huge variety and complexity makes their categorisation and in turn the conception of solutions that apply to many of them, extremely difficult.

The work presented in this thesis applies modelling and simulation techniques in order to improve the security and resilience of cyber-physical systems. This is achieved through the context of three major categories of cyber-physical systems: Critical Infrastructure – Industrial Control Systems (CI-ICSs), Wireless Sensor Network (WSNs) and Hot-Desking Systems (HDS). The selection of these categories lies in the fact that they are used in many critical cases and often with only small changes from one case to another. For each one of these categories, some reference use cases are selected and then modelling and simulation techniques are applied on them in order for their security and/or resilience perspective to be improved. The set of tools that are used for the aforementioned modelling and simulation, consists of Game Theory, Stafford Beer's Viable System Model (VSM), Epidemiology, SensomaX (a custom-made agent-based middleware), Monte Carlo predictive modelling and Event-Driven Simulation (EDS) and in every use case, one or more of them in combination are used. The presented techniques manage to tackle the issues identified in existing approaches while addressing the stated research questions and they ultimately, introduce a new way of Systems Thinking.

More specifically, in terms of the three aforementioned categories (CI-ICSs, WSNs and HDS), this thesis includes models that use Game Theory (GT), Viable System Modelling (VSM), Monte Carlo predictive modelling and epidemiology techniques in order to improve the cyber security risk management procedure in ICSs, applications of GT and auction-based algorithms, EDS and SensomaX in order to suggest solutions that improve WSNs both from a security and a resilience perspective and finally, approaches that use EDS in order to apply a HDS that can improve the productivity of an enterprise. More details on these models and the contribution of the author to them, can be found in section 1.3.

Practically the entirety of the research conducted and presented in this thesis is published in nine publications for various, peer-reviewed journals and conferences with one of them winning the Best Paper Award of its track.

AUTHOR'S DECLARATION

I declare that the work in this dissertation was carried out in accordance with the requirements of the University's Regulations and Code of Practice for Research Degree Programmes and that it has not been submitted for any other academic award. Except where indicated by specific reference in the text, the work is the candidate's own work. Work done in collaboration with, or with the assistance of, others, is indicated as such. Any views expressed in the dissertation are those of the author.

SIGNED: .. [redacted] ..... DATE:.....28 February 2019.....

ACKNOWLEDGMENTS

This PhD thesis is dedicated to my parents and my brother for always being there for me and supporting my choices. This thesis would have not been possible without their love, support, trust and motivation. I am grateful for everything they have helped me to achieve.

I would like to express my gratitude to my supervisors, Dr. Theo Tryfonas and Dr. George Oikonomou for their perpetual support, advice and guidance through the whole journey of my PhD.

I would like to thank Dr. Theodoros Spyridopoulos for his valuable advice and joint research work through this PhD.

My sincere appreciation for the great joint work, papers and collaboration through the years to Dr. Theo Tryfonas, Dr. George Oikonomou, Dr. Theodoros Spyridopoulos, Mr. Peter Cooper, Mr. Teslim Fagade, Dr. Mo Haghighi, Dr. Alexios Mylonas, Dr. Alison Burrows, Dr. Pete Woznowski and Dr. Robert Piechocki.

I would also like to thank all my friends who supported me through the years.

And finally, I want to thank Nicole for so many reasons and for always being there for me!

This work was funded and supported by the Systems Centre and the EPSRC funded Industrial Doctorate Centre in Systems (Grant EP/G037353/1) and Frazer-Nash Consultancy.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

ABC	Activity-Based Costing
AC	Attack Coefficient
AE	Agent Examiner
AES	Advanced Encryption Standard
AP	Attacker's Payoff
APT	Advanced Persistent Threat
BD	Big Data
BSR	Base Station's Reward
CH	Cluster-Head
CHR	Cluster-Head's Reward
CI	Critical Infrastructure
CI-ICSs	Critical Infrastructures and Industrial Control Systems
CIA	Confidentiality, Integrity and Availability
CIO	Chief Information Officer
CNI	Critical National Infrastructure
CPS	Cyber-Physical System
CROSS	Clustered ROuting for Selfish Sensors
DB	Database
DDoS	Distributed Denial of Service
DoS	Denial of Service
DMS	DDoS Mitigation System
DMZ	De-Militarized Zone
EDS	Event-Driven Simulation
FA	Feed Agent
GA	Global Agent
GUI	Graphical User Interface
GT	Game Theory
HMI	Human Machine Interface
HWSN	Heterogeneous Wireless Sensor Network
ICO	Information Commission Office
ICS	Industrial Control System
ID	Intrusion Detection
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IED	Intelligent Electronic Device
IoT	Internet of Things
IP	Intrusion Protection/Prevention
IPS	Intrusion Protection System
ISMS	Information Security Management System
IT	Information Technology
LA	Local Agent
LAX	Los Angeles International Airport
LEACH	Low-Energy Adaptive Clustering Hierarchy

LGCA	Localised Game-theoretical Clustering Algorithm
MTTI	Mean-Time-To-Infection
NE	Nash Equilibrium
NFV	Network Function Virtualisation
NIST	National Institute of Standards and Technology
OGC	Open Geospatial Consortium
PLC	Programmable Logic Controller
QoS	Quality of Service
R&D	Research and Development
RNOS	Requirements for Non-Obvious Solution
ROSI	Return on Security Investment
RPL	Routing Protocol for Low Power and Lossy Networks
RQ	Research Question
RTU	Remote Terminal Unit
SA	System Agent
SC	System Configuration
SCADA	Supervisory Control And Data Acquisition
SDN	Software-Defined Networking
SEIS-V	Susceptible, Exposed, Infectious, and Susceptible with Vaccination
SIR	Susceptible - Infected - Recovered
SIRS	Susceptible, Infected, and Temporarily Recovered
SIS	Susceptible - Infected - Susceptible
SMB	Small and Medium-sized Business (?)
SXCS	SensomaX Companion Simulator
TA	Task Agent
TCE	Task Core Executer
TE	Task Engine
TCE	Task Core Executer
TDDG	Trust Derivation Dilemma Game
TE	Task Engine
TSA	Transportation Security Administration
UCON	Usage CONtrol
Vensim	Ventana Simulation Environment
VSM	Viable System Model
WSN	Wireless Sensor Network
3D	Three Dimensional
2D-GTEB	Two Dimensional Game-Theoretic Energy Balance
3D-GTEB	Three Dimensional Game-Theoretic Energy Balance
6LoWPAN	IPv6 over Low-Power Wireless Personal Area Networks

I. INTRODUCTION AND LITERATURE REVIEW

Section I includes the first two chapters of the thesis. In more details, chapter 1 provides the problem statement, the aim of this work, the research questions it addresses, the published work of the author, the research design and the structure of the thesis. Chapter 2 includes the necessary background knowledge and review of the existing literature around the scientific areas that our research focuses on.

Chapter 1

INTRODUCTION

Chapter 1 provides the problem statement, the aim of this work, the research questions addressed in this thesis, a full list of publications with a short summary of what each one is about and its contribution to the literature. The research design is also thoroughly discussed in this chapter as well. A more detailed structure of this thesis is presented at the end of the chapter.

1. INTRODUCTION

Our needs are constantly becoming more and more complex. As a result, the mechanisms that cover these needs are steadily becoming more and more complex, as well. The number of parameters that these mechanisms involve is growing higher and higher to the point that not only computers are absolutely necessary in order to handle all that complexity, but there is a need for the involved procedures to be as optimised as possible in order for, even the most modern systems, to be able to provide a useful outcome or service within a reasonable amount of time. In some cases, even minor improvements on the running time, efficiency, resources needed or cost, can lead to a huge difference on the quality of the service provided or on the impact that the outcome can have on people's lives.

Additionally, due to the aforementioned situation, the variety of the existing systems and the available tools that can be used for building, understanding and tweaking them, is so big, that there is no single tool, method or mechanism to usefully apply to all of them. Both the systems and the applied tools can be categorised to so many categories and often the separating lines among them are really vague.

However, this work makes an attempt, through multiple case studies, to categorise the presented (often critical) systems and propose novel approaches for solving their important problems using each time the necessary tools. Every time, the benefits are clearly identified and discussed, analysing also what was the gap in the existing literature around these topics and what could have made these solutions even better.

1.1 Problem Statement

There are many definitions of what a system is and they tend to vary according to the field they apply on or refer to. A well-known general one is the following: "System is a set of things working together as parts of a mechanism or an interconnecting network; a complex whole." provided by Oxford Dictionaries[1]. No matter which one of them

[1] Oxford Dictionaries: https://en.oxforddictionaries.com/definition/system

someone is willing to accept, two things are sure; they are ubiquitous and keeping them safe and optimised is of major importance. In other words, their safety and resilience is, by any measure, very important. This, however, is not usually easy. As mentioned before, systems' applications and the needs that they have to cover, are constantly evolving but this is not always the case for their security or resilience mechanisms. That is because many kinds of systems exist for many years now and were built under completely different circumstances, in order to cover completely different needs and having to be protected from completely different dangers. However, as the circumstances, the needs and the threats are advancing rapidly, it is not easy for systems to keep up with the same pace, for various reasons. Two of the most common are the following.

Firstly, it is often the case that some parts of a system cannot keep evolving with the pace that some other parts of the same system do. As such, what we end up with is a system including some components significantly older than others. These redundant components, though, will often have their security issues and since, according to the previous definition, the system is "a set of things…" it will only be as safe as its weakest component.

Secondly, the huge variety and omnipresence of systems have caused some of them to be used for purposes other than the ones they were designed for. Even if that purpose is similar, the design requirements could be different enough in order for weaknesses to occur.

That variety and omnipresence though can cause another issue; systems' categorisation is neither easy nor obvious. With so many of them, so many differences and similarities among them and so much chaotically-organised research around them, it is very hard to put them into groups, such that the same security or optimisation solutions can apply for all the members of the same group and this is another reason that makes, keeping systems safe and resilient, an extremely difficult task. Making this task a bit simpler is the direction that this work aims towards, by answering the research questions that follow.

It should be highlighted that although the term "resilience" is a bit broad and vague and it can even have a security aspect, in this thesis it is used as an umbrella term to denote, every non-security aspect of a system that the presented models attempt to improve, like for example resource allocation. Another alternative term that could have

been used instead is the “Quality of Service” (QoS). However, the term resilience was chosen because it reflects better the element of optimisation (and recovery, where applicable) that is involved and also because the word “service” could create confusion in some cases.

1.2 Aim and Research Questions

As mentioned, it is very difficult to provide solutions that apply on many kinds of systems due to their extremely big variety, both in terms of components and interconnections among them but also in terms of the scope they serve.

In this thesis, we focus on Cyber-Physical Systems (CPSs) which are the systems that have both a cyber or digital dimension along with their physical one. More specifically, what we mean by the term CPSs, is the group of systems that can be compromised either physically (i.e. by physically removing some sensors from a WSN) or non-physically due to their access to the internet or a dataset/database that can be compromised remotely.

CPSs have all the characteristics (and therefore the same vulnerabilities, as well) of a system that were mentioned before. However, due to their twofold nature (cyber and physical), not only some additional vulnerabilities can be present, but mitigating these (additional or not) vulnerabilities can require unconventional, sophisticated methods that can capture the connections and relationships between the various system components. Exploring methods of improving CPSs security or resilience (as it was defined before) is the goal of this thesis and this exploration will go through answering a series of Research Questions (RQs) related to them. More specifically, these are:

- RQ1: Up to what level can the existing approaches improve the security and the resilience of Cyber-Physical Systems?
- RQ2: How can we improve the security of Cyber-Physical Systems?
- RQ3: How can we improve the resilience of Cyber-Physical Systems?

However, even the group of CPSs can include too many and sometimes too different with each other representatives, making it extremely difficult to propose methods that improve their security and/or their resilience and apply on all of them. Therefore, the research questions will be answered through the context of some sub-groups of CPSs. In order for this to be as useful as possible though, members of these sub-groups need to meet some requirements. More specifically, they should:

a) be used in many fields and cases and for many scopes
b) do so with only small changes from case to case
c) be considered of significant importance due to their use cases

As such, we are going to address the research questions through exploring:

i) Critical Infrastructures and Industrial Control Systems (CI-ICSs)
ii) Wireless Sensor Networks (WSNs)
iii) Hot-Desking systems

Exploring these types of systems is of great worth and importance not only because they meet the previous three properties but also because in conjunction with the earlier mentioned chaotically-organised research that has inevitably left essential gaps, such an exploration could lead to solutions and mechanisms that have a great range of application and solve problems that are not only critical but also neglected

Under the prism of those categories, the three RQs that were presented above, could now be further elaborated into the following research questions:

RQ1.1: Up to what level can existing tools protect WSNs?
RQ1.2: Up to what level can existing tools protect ICSs?
RQ1.3: Hot-Desking is becoming popular again. Can the traditional Hot-Desking methods keep-up with the modern businesses' needs?

RQ2.1: Can we improve WSNs security?
RQ2.2.1: Can we provide cost-efficient protection for ICSs?

RQ2.2.2: Can we improve existing risk management approaches for ICSs?

RQ3.1: Can we improve non-security aspects of WSNs?

RQ3.2: Can we improve Hot-Desking applications?

with a few more that can possibly be added. The numbering is such so that the corresponding to the initial three RQs is obvious.

Although these elaborated RQs are all answered in this thesis, it is the structure of the initial three RQs that is adopted in order to avoid causing confusion to the reader. However, the answers to all RQs are specifically pointed out throughout the thesis and also in section 5.2, in a way that, no matter what RQ (either out of the three former ones or out of the eight latter ones) the reader is seeking, it is very easy for him or her to find them.

More specifically, in terms of the three aforementioned categories (CI-ICSs, WSNs and HDS), this thesis includes models that use Game Theory (GT), Viable System Modelling (VSM), Monte Carlo predictive modelling and epidemiology techniques in order to improve the cyber security risk management procedure in ICSs, applications of GT and auction-based algorithms, EDS and SensomaX in order to suggest solutions that improve WSNs both from a security and a resilience perspective and finally, approaches that use EDS in order to apply a HDS that can improve the productivity of an enterprise. More details on these kinds of systems and elaboration on their importance, take place in their respective chapters.

The research work that is presented in the following chapters orbits around the research questions and it will be specifically mentioned throughout this work, every time that one of these is answered.

1.3 Published Outputs

Before we move on to the Research Design section, it is useful that all publications are presented (in chronological order) along with a small summary for each of them. These publications thoroughly and coherently bond the research material. It should be mentioned that all this work, was funded and supported by the Systems Centre and the EPSRC funded Industrial Doctorate Centre in Systems (Grant EP/G037353/1) and Frazer-Nash Consultancy.

From the list below, paper 3, has been awarded the Best Paper Award of its track, at IEEE Sensors 2015.

1. Spyridopoulos, T., Maraslis, K., Tryfonas, T., Oikonomou, G., & Li, S. (2014). Managing cyber security risks in industrial control systems with game theory and viable system modelling. In *2014 9th International Conference on System of Systems Engineering (SOSE)* (pp. 266–271).

This paper presents an innovative approach in the context of cyber security risk management in Industrial Control Systems (ICSs) which challenges not only the research community but the practitioners, as well. Their proprietary nature along with the complexity of those systems renders traditional approaches rather insufficient and creates the need for the adoption of a holistic point of view. This approach aims at providing cost-efficient protection solutions to the defender by combining the concepts of Viable System Model (VSM) and Game Theory (GT). During the development of this method, the proprietary and interconnected nature of an ICS was taken into consideration. VSM was not only used to capture the interconnections of the ICS's cyber components but also the relationships among the components of different ICSs. The proposed model provided cost-efficient defense strategies and at the same time demonstrated a cost-benefit cyber-security risk management process in ICSs that would require minimum informational input.

The contribution of the author of this thesis to this publication was his participation in the brainstorming and the whole set-up of the paper as well its game theoretic framework and the calculation of the Nash Equilibria.

2. Maraslis, K., Spyridopoulos, T., Oikonomou, G., Tryfonas, T., & Haghighi, M. (2015). Application of a game-theoretic approach in smart sensor data trustworthiness problems. In *IFIP International Information Security Conference* (pp. 601–615). Springer.

In this paper, Game Theory has been employed for the purposes of developing an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) model for

the protection of WSNs. The attacker's goal is to compromise the deployment by causing nodes to report faulty sensory information. The defender, who is the WSN's operator, aims to detect the presence of faulty sensor measurements (IDS) and to subsequently recover compromised nodes (IPS). With this game-theoretical approach we attempt to identify the presence of Nash Equilibria in the two proposed games. Two methods of validation have been applied in order to reveal the models' effectiveness. The results of the first one matched the results of the analytical models, while the results of the second one confirmed the detection model's effectiveness in a simulated IPv6-connected network of smart objects.

All parts of this publication were contributed by the author of this thesis, apart from the two validation methods that make use of SensomaX and Cooja.

3. Haghighi, M., Maraslis, K., Tryfonas, T., & Oikonomou, G. (2015). Game-theoretic approach towards energy-efficient task distribution in wireless sensor networks. In *2015 IEEE SENSORS* (pp. 1–4).[2]

This paper uses game-theoretical approach along with auction-based techniques for the purposes of optimising task distribution among the sensor nodes and improving energy consumption in WSNs. The proposed game-theoretical approach enabled SensomaX to allocate resources to the deployed applications, based on nodes' processing and memory availability, as well as their remaining energy level.

The contribution of the author of this thesis to this publication was his participation in the brainstorming and the whole set-up of the paper as well its game theoretic framework, its auction-based techniques and the calculation of the Nash Equilibria.

4. Haghighi, M., Maraslis, K., Tryfonas, T., Oikonomou, G., Burrows, A., Woznowski, P., & Piechocki, R. (2015). Game-theoretic approach towards Optimal Multi-tasking and Data-distribution in IoT. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 406–411). IEEE.

[2] Best Paper Award of its track, at the IEEE Sensors 2015

Existing applications often require nodes to implement logical decision-making on aggregated data, which involves more processing and wider interactions amongst network peers, resulting in higher energy consumption and shorter node lifetime. In this paper, the focus was given on improving energy consumption and optimizing task distribution amongst WSN sensor nodes by combining SensomaX and auction-based techniques and taking into account nodes' processing capability, memory availability and remaining energy level. The proposed model demonstrated that in a multitier, hierarchical WSN where there are cases that the applications are collaboratively executed by multiple clusters, then the energy consumption could be reduced.

The contribution of the author of this thesis to this publication was his participation in the brainstorming and the whole set-up of the paper as well its game theoretic framework and the calculation of the Nash Equilibria.

5. Spyridopoulos, T., Maraslis, K., Mylonas, A., Tryfonas, T., & Oikonomou, G. (2015). A game-theoretical method for cost-benefit analysis of malware dissemination prevention. *Information Security Journal: A Global Perspective*, *24*(4–6), 164–176.

This paper links Game Theory and virus proliferation models for the purposes of developing a cost-benefit approach that is able to assess defence strategies capable of mitigating malware proliferation. This work combines a game-theoretical framework with existing well-known epidemiology models (Susceptible - Infected – Recovered (SIR) and Susceptible - Infected – Susceptible (SIS)), resulting in a custom model which incorporates the ability to capture the relationships between nodes within a network, along with their effect on malware dissemination process. Drawing upon a model that illustrates the network's behaviour based on the attacker's and the defender's choices, Game Theory is employed for calculating the optimal strategies for the defender in order to minimize the effect of malware spread and the cost of security at the same time. The proposed model provides a cost-benefit risk management framework for managing and mitigating possible malware spreads.

The contribution of the author of this thesis to this publication was his participation in the brainstorming and the whole set-up of the paper as well its game theoretic framework and the calculation of the Nash Equilibria.

6. Maraslis, K., Cooper, P., Tryfonas, T., & Oikonomou, G. (2016). An Intelligent Hot-Desking Model Based on Occupancy Sensor Data and Its Potential for Social Impact. In *Transactions on Large-Scale Data-and Knowledge-Centered Systems XXVII* (pp. 142–158). Springer.

This paper presents a model development that employs occupancy sensor data in a commercial Hot-Desking environment for the better facilitation of office resources management. In this particular case, desk allocation in a Hot-Desking environment is employed, with results that outweigh the costs of occupancy detection. We explored the potential for intelligent hot desking to substantially improve productivity in the working environment compared to the traditional hot-desking systems. It has been verified, that occupancy-based smart building concepts, can not only be valuable, but at the same time operationally practical.

This publication was contributed almost solely by the author of this thesis.

7. Fagade, T., Maraslis, K., & Tryfonas, T. (2017). Towards effective cybersecurity resource allocation: the Monte Carlo predictive modelling approach. *International Journal of Critical Infrastructures*, *13*(2–3), 152–167.

This work demonstrates why using conventional risk assessment approach as budgeting process can result in significant over/under allocation of resources for cyber capabilities. Instead, the proposed Monte Carlo predictive simulation model can serve as a benchmark for policy and decision support to aid stakeholders in optimizing resource allocation for cyber security investments.

The contribution of the author of this thesis to this publication was his participation in the brainstorming and the whole set-up of the paper as well the validation procedure of the Monte Carlo approach.

8. Spyridopoulos, T., Maraslis, K., Tryfonas, T., & Oikonomou, G. (2017). Critical infrastructure cyber-security risk management. *Terrorists' Use of the Internet: Assessment and Response*, *136*, 59.

This paper presents an alternative tactic on approaching ICSs using VSM and Game Theory. These two tools are combined in order for a holistic risk management

process that would take into account all the interdependencies among the critical components of an ICS to be developed. As a result, the proposed model avoids the commonly inherited weaknesses of existing approaches that are caused by incomplete data sets or estimation mechanisms that are not specifically designed for ICSs but are rather adaptations of traditional and often redundant approaches.

The contribution of the author of this thesis to this publication was his participation in the brainstorming and the whole set-up of the paper as well its game theoretic framework and the calculation of the Nash Equilibria.

9. Cooper, P. B., Maraslis, K., Tryfonas, T., & Oikonomou, G. (2017). An intelligent hot-desking model harnessing the power of occupancy sensing data. *Facilities*, *35*(13/14), 766–786.

This paper's aim was to develop a model based on employee's occupancy data in a hot-desking environment. More specifically, to calculate and take a decision of which desk needs to be allocated to each employee by the time of arrival. This decision is taken based on the projects that all the employees are working on at that specific point of time, and not only taking into consideration the project of the particular employee that should be assigned with a desk. The purpose of this work was not only for employees to be as productive as possible, but also for the organization to be benefited from this model development as the employees will be working under the most optimal working environment and at the same time the number of desks will be reduced. The proposed model is compared to some theoretically ideal but practically impossible models in order to demonstrate that our model produces results directly comparable to the ideal ones and feasible at the same time.

This publication was contributed almost solely by the author of this thesis.

10. (To be submitted) - Maraslis, K., Haghighi, M., Tryfonas, T., & Oikonomou, G. Game-theoretic and Auction-based Algorithms towards Autonomous Decision-making in WSNs.

In this paper, we introduce a novel approach using game theoretic and auction-based techniques in order to optimise task distribution and data gathering in WSNs. We implement and evaluate the proposed model on SensomaX, which is an agent-based,

adaptive dynamic middleware aimed at seamless integration of computational algorithms for multitasking in large-scale sensor networks. Additionally to our similar, previously published work, this one also confirms the reduction of agent processing time, when our algorithms are applied.

The contribution of the author of this thesis to this publication was his participation in the brainstorming and the whole set-up of the paper as well its game theoretic framework, its auction-based techniques and the calculation of the Nash Equilibria.

1.4 Research Design and Methodology

In this section, the whole exploration that was mentioned in the previous section, will be further analysed and justified, starting from the reasons that CI-ICSs, WSNs and Hot-Desking, were the chosen models.

As mentioned in section 1.2 these reasons are the following:

a) they can be used in many fields and cases and also for many scopes
b) they can do so with only small changes from case to case
c) they are considered of major importance due to their use cases (more on that in the chapters to follow)

There is also an extensive set of tools that are used in this work, and these tools are Game Theory, VSM, Epidemiology, SensomaX, Monte Carlo Simulation and traditional Event-Driven Simulation, for reasons that are directly related to the paradigms they are applied on. For example, Game Theory is considered a state-of-the-art tool that can effectively model a situation where the participants have antagonistic motives. VSM can successfully capture the multiple interdependencies of a system's components which essentially cancels the need to study multiple scenarios since an alteration of some interdependencies is still captured and it does not have to lead to a different case-study. Epidemiology is a very effective, holistic tool that can easily be tweaked to cover a plethora of use cases. SensomaX is a custom tool, developed by Mo Haghighi (co-author of some of the pieces of published work that are reflected in this thesis) and as such, even

core changes were possible in order to make the model cover the needs of our research in the best possible way. Monte Carlo simulation is great in viably handling uncertainty which is crucial in a decision-making process and finally, traditional Event-Driven Simulation (EDS) is exactly the needed insightful, easily modifiable tool to handle the simulation required about Hot-Desking and provide meaningful, well-presented results. The suitability of these tools is more extensively justified in the following chapters, where these tools are put in use.

Risking oversimplification, we could categorise these tools in two main categories: Modelling (GT, VSM and Epidemiology) and Simulation (SensomaX, Monte Carlo, EDS). Roughly speaking, we could say that modelling offers great insight to systems with their cyber side more dominant (instead of their physical one) while simulation achieves the same for systems with their physical side more highlighted. Although both of these categorisations (i.e. modelling/simulation and cyber/physical) are risky because the involved categories' respective boundaries are often extremely vague, they are helpful in order to demonstrate the wide range of the applications presented, the rationale behind choosing them and finally to help us extract some useful patterns and conclusions.

The whole work that is presented in this thesis consists of smaller pieces of work that have all been published (papers 1-9). Table 1 demonstrates the correspondence among these papers and the aforementioned tools and categories followed by the full list of published papers (that was presented also in section 1.3) for better visibility.

Table 1: Categorisation of publications based on their fields of application and used tools

		Categories		
		CI-ICSs	WSNs	Hot-Desking
Tools	Game Theory	1, 5, 8	2, 3, 4	
	VSM	1, 8		
	Epidemiology	5		
	SensomaX		2, 3, 4	
	Monte Carlo	7		
	EDS			6, 9

Since the numbers in Table 1 and Figure 1 correspond to the published work, the publication list is mentioned below again, for convenience.

Published work

1 Spyridopoulos, T., Maraslis, K., Tryfonas, T., Oikonomou, G., & Li, S. (2014). Managing cyber security risks in industrial control systems with game theory and viable system modelling. In *2014 9th International Conference on System of Systems Engineering (SOSE)* (pp. 266–271).

2 Maraslis, K., Spyridopoulos, T., Oikonomou, G., Tryfonas, T., & Haghighi, M. (2015). Application of a game-theoretic approach in smart sensor data trustworthiness problems. In IFIP International Information Security Conference (pp. 601–615). Springer.

3 Haghighi, M., Maraslis, K., Tryfonas, T., & Oikonomou, G. (2015). Game-theoretic approach towards energy-efficient task distribution in wireless sensor networks. In *2015 IEEE SENSORS* (pp. 1–4).

4 Haghighi, M., Maraslis, K., Tryfonas, T., Oikonomou, G., Burrows, A., Woznowski, P., & Piechocki, R. (2015). Game-theoretic approach towards Optimal Multi-tasking and Data-distribution in IoT. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (pp. 406–411). IEEE.

5 Spyridopoulos, T., Maraslis, K., Mylonas, A., Tryfonas, T., & Oikonomou, G. (2015). A game-theoretical method for cost-benefit analysis of malware dissemination prevention. *Information Security Journal: A Global Perspective*, *24*(4–6), 164–176.

6 Maraslis, K., Cooper, P., Tryfonas, T., & Oikonomou, G. (2016). An Intelligent Hot-Desking Model Based on Occupancy Sensor Data and Its Potential for Social Impact. In *Transactions on Large-Scale Data-and Knowledge-Centered Systems XXVII* (pp. 142–158). Springer.

7 Fagade, T., Maraslis, K., & Tryfonas, T. (2017). Towards effective cybersecurity resource allocation: the Monte Carlo predictive modelling approach. International Journal of Critical Infrastructures, 13(2–3), 152–167.

8 Spyridopoulos, T., Maraslis, K., Tryfonas, T., & Oikonomou, G. (2017). Critical infrastructure cyber-security risk management. *Terrorists' Use of the Internet: Assessment and Response*, *136*, 59

9 Cooper, P. B., Maraslis, K., Tryfonas, T., & Oikonomou, G. (2017). An intelligent hot-desking model harnessing the power of occupancy sensing data. *Facilities*, *35*(13/14), 766–786.

To be submitted

10 Maraslis, K., Haghighi, M., Tryfonas, T., & Oikonomou, G. Game-theoretic and Auction-based Algorithms towards Autonomous Decision-making in WSNs.

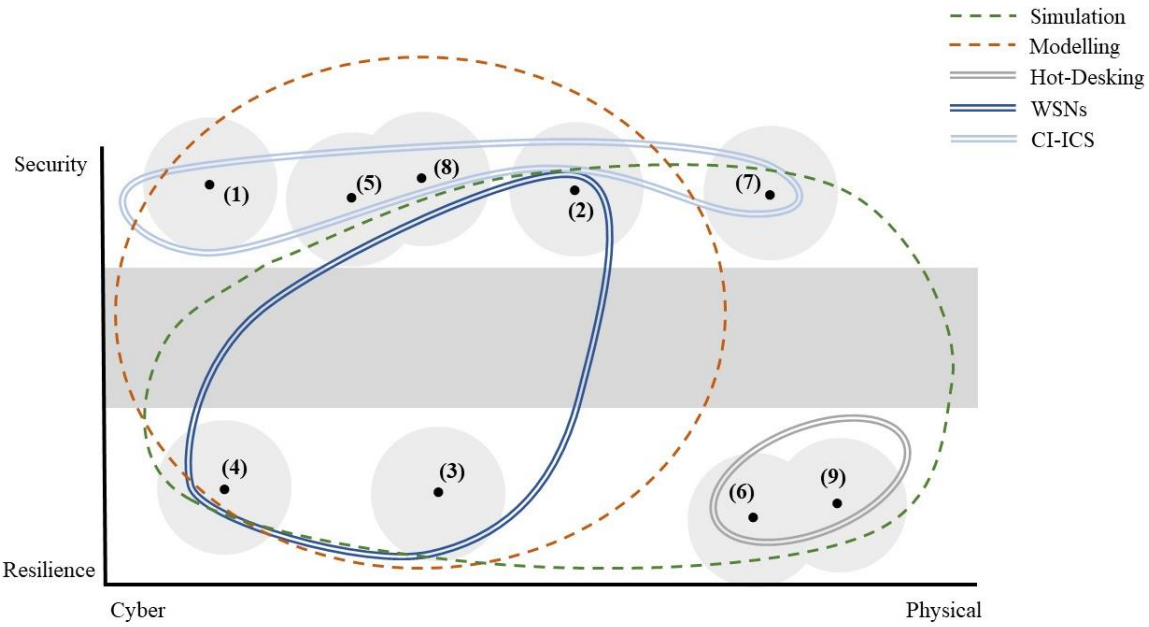


Figure 1: Graphical representation of applications' classification

Figure 1 depicts an additional categorisation of the publications, this time reflecting the orientation of the proposed models (Security or Resilience, where resilience is defined on page 5) and the nature of the systems that these models are applied on (Cyber or Physical). Once more, it needs to be emphasised though that the boundaries of such categories are sometimes very vague. This is especially obvious in the case of the nature of the systems and that is due to the fact that the involved systems have both cyber and physical subsistence (since they are CPSs). Therefore, many of the dots on Figure 1, could have also been placed elsewhere, although still close to their current position. As far as the presented applications' orientation is concerned, we have established from the beginning a strict disunion between the resilience-oriented applications and the security-oriented ones, which also led to the creation of the logic of the chapters of this thesis. Due to that, in Figure 1 we did not expect to see any dots/papers within the grey horizontal zone in the middle of the graph. Therefore, in order for this work to be able to claim that studies a range of relevant systems that is as wide as possible, the dots of Figure 1 should cover an area as wide as possible. As one can easily surmise from the graph, this is indeed the case! Additionally, since the horizontal position of most dots could be slightly different, a light grey circular field has been drawn around every dot depicting an approximation of

the area within which it could have been moved. It is apparent that these fields cover a significant portion of the remaining area (apart from the aforementioned grey horizontal zone) which is another indication of the thoughtful selection of the case-studies that are presented in the following chapters and in general the wide field of application of the proposed research models.

Finally, another useful observation that Figure 1 can lead to is the, essentially obvious by definition, overlap of modelling and simulation.

1.5 Structure of Thesis

The rest of the thesis is structured as follows:

Chapter 2 includes some necessary background knowledge on the scientific areas that the proposed work belongs to as well as a review on the related literature. In addition, in this chapter the research gaps of the existing approaches are presented along with the benefits of the proposed ones.

Chapter 3 provides the proposed models on improving WSNs and CI-ICSs from a security and risk management perspective, along with the research findings. The work documented in this chapter has been peer-reviewed and published in papers 1, 2, 5, 7 and 8 from the list of papers in section 1.3.

Chapter 4 includes the proposed models on improving WSNs from a non-security perspective (energy efficiency, packet loss and processing time) and a novel application on using Hot-Desking in order to increase productivity in a work environment. The work documented in this chapter has been peer-reviewed and published in papers 3, 4, 6, 9 and 10 from the list of papers in section 1.3.

Chapter 5 summarises the research contribution, discusses the way that the research questions have been addressed and concludes the thesis.

Chapter 2

Background Knowledge and Literature Review

Chapter 2 includes the necessary background knowledge on the scientific areas that the proposed research work focuses on, as well as a review of the existing literature around the areas of Systems' Security and Risk Management and also Systems' Resilience and Optimisation. This chapter also identifies the gaps of existing literature while answering RQ1. Finally, it provides the benefits of our proposals compared to the existing research approaches.

2. Background Knowledge and Literature Review

This chapter includes, in its first part, some necessary background knowledge about the work that is going to follow and a review of the related literature in its second one.

2.1 Introduction

In this section, there is firstly, some background knowledge that the reader needs to know in order to be able to follow the literature review that is presented later in this chapter and the contribution which begins in the next chapter. Although much information could qualify to be included in background knowledge, only the more technical parts that are about some used tools will be established here. The remaining necessary background knowledge will be established in the, each time, corresponding chapter or section.

2.2 Background Knowledge

The necessary technical knowledge about Viable System Model, Game Theory and Epidemiology is presented in this section.

2.2.1 Viable System Model (VSM)

The Viable System Model was firstly introduced by Stafford Beer in 1972.[1]. VSM models the organisational structure of viable and autonomous systems. The model initially divides the enterprise in three fundamental parts (Operations, Management and Environment), which are connected to each other in order to maintain the viability of the whole system.

As presented in Figure 2, an enterprise, composed of the operational and management parts, entails five different systems that communicate with each other and the environment. The presence of those systems along with the interrelationships between

them and their communication with the corresponding environment, preserve the viability of the enterprise.

System 1 refers to the operational units within the enterprise. Each unit can communicate with other operational units and the external environment, transferring and receiving data. The overall coordination of System 1's operations is managed through System 2. The control of System 1 is carried out by System 3, while System 3* is responsible for auditing the operations in System 1. Each operational unit within System 1 has its own management system, exchanging data with it and forming a new VSM inside the initial VSM.

System 2 is responsible for the coordination of the activities of the operational units that form System 1. It also communicates with System 3 in order to transfer the results of its coordination actions.

System 3 manages the units of System 1, controlling their behaviour by having access to all of them. It is also responsible for the provision of synergies among the operational units. It receives the coordination-related data from System 2 and the results of the audit conducted by System 3* in order to take new decisions regarding the management of System 1. It also communicates with System 4, which dictates the changes that should be made due to the ever-changing external environment.

System 3* audits the operational units of System 1 in order to identify whether System 3's management commands are followed by the operational units and whether changes should be made for the System 1's performance improvement.

System 4 communicates with the environment in order to identify changes in it and propose certain approaches to System 5 for the whole system's evolution. It also communicates System 5's decisions to System 3.

System 5 is the upper level of the management part of the VSM. It deals with the policies of the enterprise and its role within the environment. It communicates with System 4 in order to receive information regarding the changes in the environment. After deciding the changes that have to take place in the operational part of the enterprise, it delivers them to System 4. System 5 also monitors the homeostasis between System 4 and System 3 and receives information from System 3 regarding the current status of the system. Ultimately, System 5 is the one responsible for the long-term decisions.

In our proposed model, we make use of the systemic approach that the VSM embodies in order to construct a formal method for the evaluation of cyber components in the complex environment of Industrial Control Systems (ICSs). By identifying the purpose of each cyber component and the dependencies that are created, according to the VSM structure, we unveil the real dimensions of the consequences of its disruption or destruction. In addition, its recursive nature that dictates a VSM to be composed of other VSMs and, at the same time, be part of a wider VSM in a system of systems way gives us the ability to explore interdependencies between various ICSs.

VSM will be a very important tool for us in the chapters to follow.

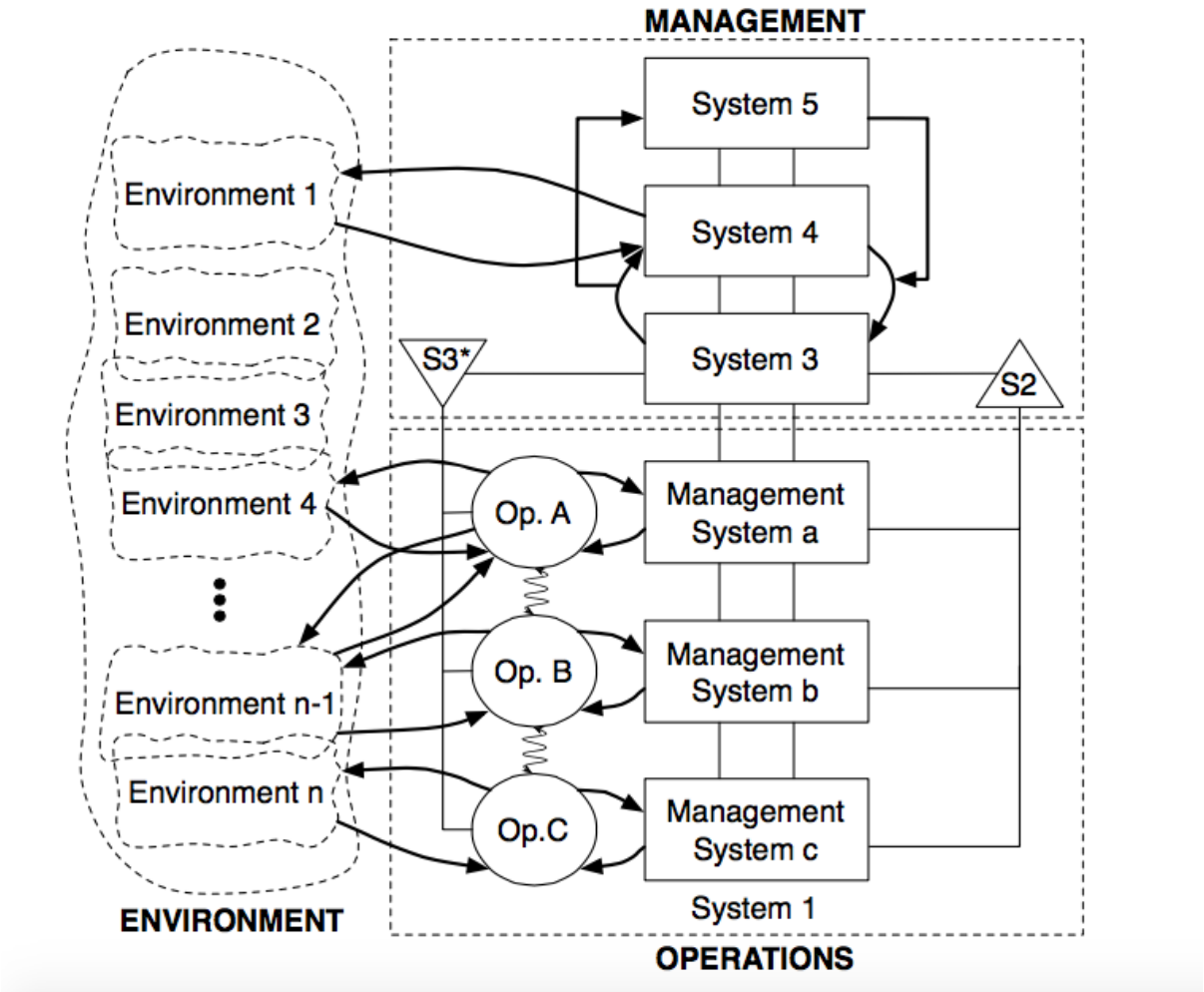


Figure 2: The Viable System Model

2.2.2 Game Theory

Game theory is a tool that is applied more and more on numerous problems and various scientific fields. It is considered to be a modern approach suitable for situations where adversarial strategies and conflicting interests take place [2][3]. In particular, Game Theory is used to describe scenarios where decisions need to be made by multiple contestants. Every combination of all contestants' decisions corresponds to a possibly different reward for each of them. Those contestants are called players and the whole scenario, including all the possible actions (that are called strategies) and the rewards (that are called payoffs), is quantified and is considered a game. One of the basic assumptions that apply on such games is that the players are considered to be rational in a sense that they will decide about their actions based exclusively on their aim to maximise their reward and that they are generally risk-averse. It should be noted that reward/payoff can also be a negative number. In this project, it is assumed that an unknown payoff can be either positive or negative unless it is explicitly mentioned otherwise or if it is called "loss" which implies that the aforementioned payoff is negative [4].

There are different approaches available for a game that depends on the kind of the game itself. The basic kinds of games along with the characteristics that a game needs to have in order to belong to each of those categories are demonstrated below.

Cooperative/Non-cooperative Games

A game is called cooperative when players do not care about maximising their individual payoff as is the case with the non-cooperative ones. Instead, the goal is the maximisation of the overall payoff. As far as the research area of network security is concerned, the games usually include players with conflicting interests (e.g. attacker and defender) and thus they mostly fall into the category of non-cooperative ones since no kind of collaboration can exist between an attacker and a defender [5].

Perfect/Imperfect Information Games

A game is considered to be a perfect information one when every player knows all the strategies that all the other players have already followed before, as part of the same game. If this principle does not apply to all players or all past strategies, then the game is considered of the Imperfect information type [2].

Complete/Incomplete Information Games

As in the perfect and imperfect information games, the division between complete and incomplete information games is made based on the amount of information that is known by the players. If every player is aware of the available strategies and payoffs of all the players in the game, then this game can be considered a complete information one. If this is not the case for every player all for all strategies/payoffs then it is considered to be an incomplete information game. This category should not be confused with the previous one (complete / incomplete information). The distinction lies in the fact that the actions, which are the strategies already followed in the past, are not taken into account in this category although they consist an important characteristic of the previous one. What every player is only required to know in order for the game to be treated as a complete information one is the payoffs and all the available strategies of the players, without the ability to be aware of which of those strategies has been chosen, by whom and when [2].

Static/Dynamic Games

In static (or one-shot) games all players choose a strategy simultaneously in the beginning of the game and they cannot change it throughout the whole game. Dynamic games, on the other hand, allow the players to change strategies while the game is in progress [5].

Iterated/Non – iterated Games

Iterated games are the ones that are comprised of more than one iterations while the non- iterated ones consist of a single iteration. It should be noted that an iterated game can be either a static or a dynamic game while a non-iterated can only be a static. That holds because there is a chance that a game consists of many iterations but the players are not allowed to change their initial strategy after the game has started. In this case, the game is typically considered iterated (although from a solver's view all iterations can be considered as one single iteration) but it is also static [6].

Constant/Non-constant-sum Games

Games where the sum of the payoffs of all players is always equal to a constant, are constant sum games. In any other case, the game is a non-constant one. Zero-sum games constitute a subcategory of constant sum games that consists of the games where the sum of the payoffs of all players is always equal to zero. That of course entails that if not all payoffs are equal to zero, there is at least one player with negative payoff [7].

In positive sum games (i.e. constant sum games for a positive constant), some players can take advantage, which means raise their payoff, due to the actions chosen by all players, even if some of them benefit more than the others. In this way, there can be some players loosing when other players are winning while there is an overall gain. On the other hand, in a negative sum game each player can cause loss to both themselves and the other players and end up with a loss in total.

When a game theory problem is investigated, it is firstly quantified so that it is brought to a form like the one described above; with strategy sets and payoffs for all possible combinations of them. Afterwards, a solution to this problem is found. The notion of "solution" to these kinds of problems could take many forms. Some of the most popular are demonstrated below.

Maximin and Minimax

Maximin and Minimax strategies are very important in Game Theory and especially in two player, zero sum games which is the kind of games that will be investigated in this work. The maximin strategy is the one that the player whose payoffs correspond to the payoff matrix elements should follow in order to receive the maximum possible payoff in the worst case scenario where the opponent chooses the best strategy with respect to their own benefit. In other words, maximin strategy will lead the aforementioned player to the maximum guaranteed payoff that this player can get. Similarly, the minimax strategy is the one that the player whose payoffs are the opposites of the elements of the payoff matrix elements should follow in order to ensure that the opponent will receive the least possible reward under the assumption that this opponent has chosen the best possible strategies with respect to their reward. Equivalently, the minimax strategy is the strategy that will ensure the aforementioned player that the opponent will receive the worst guaranteed payoff.

Of course, there can be strategies that could enable a player to receive a payoff even greater than the one that corresponds to the maximin strategy, but the crucial clue is that in this case this payoff is not guaranteed and therefore it could also be lower than the one that the worst payoff that the maximin strategy would result in. Since it is assumed that involved players are rational and thus risk-averse, it can be claimed that the maximin strategy would be preferable. The equivalent logic applies for the minimax as well [8].

Pure Nash Equilibrium

Pure Nash Equilibrium (NE) is a set that consists of one strategy of every player. These strategies are called optimal strategies and this set leads to a payoff for each player such that if any of them decides to change strategy unilaterally, then the new set of strategies will produce a payoff for the player that changed strategy that is not bigger than the one that the previous set produced. A game can have more than one Pure Nash Equilibria and in this case all of them will lead to the same payoff for all players. In the special case of a two player, zero sum game, the Pure Nash Equilibrium, if it exists, is unique and the payoff of the player that is measured (it is usual that only one player's

payoff is measured since the other player's payoff is the exact opposite) is called value of the game. In addition, where a Pure Nash Equilibrium exists, the two strategies that constitute it are the maximin and the minimax.

Mixed Nash Equilibrium

In the case of pure Nash Equilibrium, the optimal strategy denotes that the corresponding player should follow this strategy throughout the whole game in order to achieve the best guaranteed payoff. If the players were allowed to choose not only an individual strategy but a set of those and they were also allowed to attach a probability to each individual strategy of this set which would correspond to the probability that this strategy would be followed in the game (this implies that all those probabilities should add up to 1), then this set with its attached probabilities would lead to the best payoff of every player and all players' aforementioned sets co-create what is called Mixed Nash Equilibrium. As before, the best payoff of a player is considered to be the highest among the payoffs that this player could achieve by unilaterally changing strategy [5].

Game Theory will be a very useful tool in the chapters to follow, applied with solid results on areas that it is not well known for.

2.2.3 Epidemiology

This section presents the mathematical specification of the two commonly used epidemiology models SIS and SIR on which the developed model is also based. In general, such models are formulated over a fixed-size network. Nodes represent individuals and links or edges between nodes represent contacts between individuals. The infection spreads along direct links between nodes and the network is assumed to be symmetric, so that no preferential direction of the malware proliferation exists.

The SIR Model

In the SIR model [9][10][11], the total population is divided into three parts: i) susceptible nodes (denoted by S), ii) infected nodes (denoted by I) and iii) recovered nodes (denoted by R). The differential equations (1), (2) and (3) describe the rate of change of the susceptible nodes, infected nodes and recovered nodes respectively over time [12]. Here, β denotes the infection rate (i.e.: the rate at which an infected node infects other nodes within the network, or in other words, the probability that a susceptible node gets infected by an infected one, when these two come in contact), γ denotes the recovery/immunization rate (i.e.: the rate at which infected nodes are recovered/patched within the network or in other words, the probability that an infected node gets recovered from an infection and becomes immune thereafter). In this work a contact is considered as a network link between two nodes and as all nodes are connected to one another (directly or through a number of hops depending on the network's topology), they are always in contact with each other.

$$\frac{dS}{dt} = -\beta IS \tag{1}$$

$$\frac{dI}{dt} = \beta IS - \gamma I \tag{2}$$

$$\frac{dR}{dt} = \gamma I \tag{3}$$

The SIS Model

In the SIS model, the total population is divided in two parts, susceptible nodes (denoted by S) and infected nodes (denoted by I). Equations (4) and (5) model the rate of change of susceptible nodes and infected nodes respectively over time [13]. Again, β is the infection rate and this time γ is the recovery/disinfection rate. Even though the term "recovery rate" is used in both the SIR and the SIS model, it is used for slightly different purposes. In the first case recovery rate refers to immunization (the recovered node cannot

be reinfected), while in the latter it refers to disinfection (the recovered node can be reinfected).

$$\frac{dS}{dt} = -\beta IS + \gamma I \tag{4}$$

$$\frac{dI}{dt} = \beta IS - \gamma I \tag{5}$$

Both of these models will later be compared to a third one, which is custom made by us in order to cover the needs of our research.

The next section of this chapter is a short review of the literature related to our work and Systems Security and Risk Management.

2.3 Literature Review

In this section, there is a summary of the existing literature around the subjects and scientific areas that our work is based on. The reasoning behind the choice of the presented projects is that they manage to be close, or somewhat close, to the logic and practices of our proposed models that will be analysed later, while, at the same time, provide a good demonstration of the different kinds of applications that such models can be applied on.

The presented literature is split in two main categories. The first one is about the security and risk management perspective of systems and therefore, the research that is included in this category will mostly aim at providing some kind of security-related benefit to the applied system. The second category is about projects that optimise some aspect of a system, other than its security (although sometimes other aspects can have an impact on the security, as well).

2.3.1 Systems' Security and Risk Management

As mentioned, this section is about similar security-related literature applied on systems. This section is, in turn, split in more categories that correspond to the categories of the chapters to follow. There is a category about managing CI-ICSs using GT and/or VSM, another one about systems' security and risk management using Monte Carlo predictive modelling, later a category about Game Theory on WSNs' security and finally the part about Epidemiology and malware dissemination within a system.

2.3.1.1 Managing CI-ICSs using Game Theory or VSM

Managing cyber security risks in conventional Information Technology (IT) infrastructures usually follows certain established approaches [14][15]. In general, following the ISO/IEC 27005 standard on Information Security Risk Management, the methodology adopted by those approaches comprises four discrete phases and each phase consists of straightforward steps [16]:

Phase 1: Information Security Risk Identification

- Assets identification.
- Identification of cyber threats.
- Identification of existing security controls.
- Identification of vulnerabilities.
- Identification of consequences in case a vulnerability is exploited by an identified threat.

Phase 2: Information Security Risk Analysis

- Impact assessment.
- Assessment of cyber security incident likelihood.
- Level of risk determination.

Phase 3: Information Security Risk Evaluation

Risks are evaluated as the product of the impact of a cyber security incident and the likelihood of that incident.

Phase 4: Information Security Risk Treatment

The last step encompasses the proposal of risk mitigation mechanisms that will retain risks in acceptable levels or even avoid them.

Traditional approaches towards cyber security risk management in ICSs follow this methodology most of the times, adapting it to the needs of an ICS. However, as described by the authors in [17] and [18], the fact that this methodology originally focuses on IT infrastructures makes such approaches inapplicable in the complex environment of ICSs. Towards this direction many researchers have proposed methods that follow a holistic point of view in the ICS cyber security risk management process. More particularly, in [19] the authors adopt a mixed holistic-reductionist approach for the impact assessment of cyber-attacks. The proposed conceptual methodology, models' heterogeneous systems and evaluates the impact of an attack through the definition of different agents and their dependencies. However, although it can identify emerging interconnections, its complexity due to the lack of a unified approach towards the definition of interconnections renders it un-manageable when more details are added. The complexity also rises from the fact that it models each attack separately.

Another approach is presented in [20] where the authors use the VSM in order to examine strategic cyber security attacks that an adversary could use in order to strike the viability of an organisation. By modelling traditional cyber-attacks as attacks against the various systems that compose the VSM of the organisation, they managed to analyse the available attack tactics and their possible use for effectively attacking an organisation. Although this study does use VSM for security-related purposes, it emphasises on the attacker's perspective and therefore its scope is not to provide a tool that the defender can use, even if some of its content can be used towards this direction.

Authors of [21] build on the knowledge from models [22] and [23] about software assistants IRIS and ARMOR respectively, in order to come up with GUARDS, a novel game-theoretic approach that is used by Transportation Security Administration (TSA)

for security-related resource-limited allocation tasks regarding the protection of 400 airports of the United States. Unlike the previous two models, it can handle heterogeneous security activities and multiple diverse threats, with an almost decentralized method (meaning that headquarters do not plan a common strategy for all airports) that can take into account multiple security layers simultaneously while attempting to protect a set of targets. This project solves the game by finding its mixed Nash Equilibria. Although it is a robust model, it considers the airports almost autonomous to each other and not as systems within a larger system (TSA) making the adoption of a centralized solution that could respect the specificities of the airports, impossible.

Similarly, in [24], another airport (Los Angeles International Airport – LAX) is under investigation and ARMOR is adopted to convert the problem of optimally using their security resources (i.e. checkpoints on the roadways entering the airport and canine patrol routes) into a solvable one where mixed Nash Equilibria can be found. Although, the resources are composed of two factors, ARMOR can only focus on one of them per application.

A game-theoretical approach applied to a Critical Infrastructure is demonstrated in [25]. The authors examine a scenario where, in a smart grid with state estimators that are supposed to accurately measure the price of electricity at any given time, an attacker tries to inject faulty data while a defender tries to withstand the attacks. Those behaviours are modelled as two-player, zero-sum games, the Nash Equilibria of which need to be found. The results are then validated with simulations. However, this method lacks the element of Risk Evaluation where the possibilities of a successful attack would depend on additional parameters that would make the model more realistic.

Game-theoretic approaches are not new to Risk Analysis [26], however they are far from being used as state of art, despite various authors demonstrating how they can offer a deep insight into the problem, as they can be “mutually reinforcing” approaches [27].

In [28], the authors presented a conceptual recursive model of secure ICS that is capable of identifying the cyber security threats and take responsibility on decision-making against them using the principles of the VSM. In order to be able to have a better view of the critical sections of the ICS networks, a secure network design model has been proposed. According to the authors, academic research mostly put emphasis on the

sophisticated attacks and their mitigation techniques rather than on how to simplify security best practices. In order to address this gap, they introduce their framework which would identify feasible best practices in a simpler way. By introducing security in ICSs and by integrating the expertise of security and control systems, it would be possible to mitigate security risks and attacks. In addition, since IT controls were introduced in industrial processes, many best practice models are based on isolation. This is another one of the few projects that use VSM on ICSs security. However, its primary goal is to simplify existing practises instead of emphasising on improving them or implementing them in more holistic security framework.

Elements of originality

The content of this section is part of the answer to RQ1 by summarising the gaps of existing literature on CI-ICSs security and our addition on it. The actual additions consist part of the answer to RQ2, a more detailed response of which can be found in section 3.3.1.1, 3.3.1.2, 3.3.2 and 3.3.3.2 where our approach and its novelty are explained.

A very common problem regarding systems' security (and more particularly on ICSs) and risk management is the lack of consideration for the multiple interdependencies within the system. Other common problems include that, very often, adopted methods are just adaptations of security mechanisms not specifically designed for their use-cases or that the involved likelihood estimations are estimations or even guesses, based on past experience or incomplete sets of data.

The proposed approach that will be presented in chapter 3 not only takes into account the aforementioned interdependencies by using VSM, but also applies Game Theory which leads to the identification of Nash Equilibria in a way that considers multi-dimensional strategy sets, both for the attacker and the defender. What we end up with, is a holistic approach that focuses on improving existing security mechanisms and can take into account more complex attacking methods (like zero-day attacks) and emphasises on providing the defender of the system with a decision-making instrument that will best

protect his interests. Traditional security and risk management techniques, even those that are not only based on fixed patterns for well-documented dangers, cannot address situations like these and to the best of our knowledge there is no other research work that combines VSM and Game Theory, in a similar scheme.

2.3.1.2 Systems' Security using Monte Carlo predictive modelling

There are several works [29][30][31][32], that evaluate the budgetary allocation problems of information security investments, in an attempt to justify optimum security investment decisions. The work in [33] showed how system vulnerability can be reduced through security patches. A game-theoretic model was developed to study the strategic interaction between a vendor and a firm in balancing the costs and benefits of patch management. The approach presented by [34] is based on expected utility value of investment in order to determine the optimal investment amount. The approach suggests that the level of investment for asset protection depends on the vulnerability of the asset and associated potential losses. The work further assumes that with increase information security investment, probability of security breach decreases but marginal improvement on security also decreases with higher investment. Hence, risk averse management may maximise the expected utility of a budget to determine the maximum amount to invest, which should not exceed the potential loss of breach. The approach presented [35], uses the term 'Return on Security Investment' (ROSI), which is similar to the traditional accounting figure. The approach incorporates one-time costs and benefits of information security while it discards running costs and benefits as well as non-financial security measures. In order to support investment decisions. ROSI is calculated as: $ROSI = (Risk\ Exposure \times Risk\ Mitigation - Solution\ Costs)$ / (Solution Costs) and $Risk\ Exposure = ALE \times ARO$ where ALE denotes annual loss exposure while ARO denotes annual rate of occurrence.

In a work presented by [36], information security investment decision is based on a balanced scorecard performance measuring system. This method, in its original context evaluates organisation business performance from the angle of financial, customer, internal process and innovation. The authors extended and applied balanced scorecard method in the context of information technology to support management decisions. The

approach uses goal measurement to establish investment needs. Goal importance e.g. server downtime reduction is weighted relative to other goals in order to set goal fulfilment minimum average degree. If an investment's average degree is considered to be above the threshold, then it is deemed economically viable. This approach considers all financial and non-financial mitigation measures.

Elements of originality

The content of this section is part of the answer to RQ1 by summarising the gaps of existing literature on CI-ICSs security and our addition on it. The actual additions consist part of the answer to RQ2, a more detailed response of which can be found in section 3.3.1.1, 3.3.1.2, 3.3.2 and 3.3.3.2 where our approach and its novelty are explained.

The aforementioned research works are based on traditional predictive modelling approaches where cost estimations regarding assets tend to become unreliable, especially as the complexity increases. We applied Monte Carlo simulation in the context of information technology and more specifically on security resource allocation decisions and proposed a model that is based on a single-block optimal allocation at organisational level. This approach uses a probabilistic simulation and as a result it simplifies the cost estimation process while allows us to have a great insight of the system it is applied on. A big advantage of the adopted method is that it replaces the otherwise deterministic estimates of uncertain values about asset breach costs with a variable following triangular distribution. This distribution is one of the most commonly used in the case of limited or absence of historical data. As a result, the outcome is again probabilistic, including but not limited to the three main scenarios (best, most likely and worst case) and allowing the benefits of such type of result (i.e. better understanding of the impact of the involved parameters, confidence levels, easier sensitivity analysis if needed etc) which will ultimately lead to more accurate resource allocation on security investments and in turn, to improved security.

2.3.1.3 Game Theory on WSNs security

Game Theory has been used in the past for simulating and solving security-related problems in WSNs. For example, in [37] the behaviour of a system under a Distributed Denial of Service (DDoS) attack is under investigation based on previous work of [38]. The target environment there is a network, however the model is generic and based on the same networking principles that apply to WSNs. The attacker aims to perform a DDoS attack at a system that has implemented a firewall. The attacker's strategy is defined by the number of occupied nodes and the distribution according to which she transmits malicious traffic. The defender on the other hand can control the settings of the system's firewall. This situation was modelled as a two-player, static, non-cooperative, zero-sum game. The research concludes with suggestions for the strategy of the defender which maximise the minimum payoff of the defender regardless of attacker's decision and behaviour.

Authors in [39] try to improve the security and energy efficiency of a WSN by applying a reputation system on its nodes where low-reputed ones are shut down. Every node can improve its reputation by forwarding incoming packages. However, this forwarding causes draining of their batteries. Since conflicting interests are present, a game-theoretic model is adopted in order for the maximum possible battery life of the nodes to be assured while sustaining an unproblematic operation. In addition, there are malicious nodes that can cause package drops, making the proper flow of data even more difficult. On all scenarios of the WSN games of this work, the authors solve the problem by finding the network's Nash Equilibria. Under the assumption that the involved players are rational, the authors find the optimal strategies for both the defender and the attacker that ensure an upper limit for the expected losses when they are followed. As far as the security and power conservation are concerned, the network improves significantly in all three cases, comparing to the scenario were the game-theoretic model was not applied.

Authors of [40] investigate the case where a clustered WSN is under attack. In this project, the attacker targets the Cluster-Heads (CHs) in an attempt to crowd the data flow or drop it. The underlying Intrusion Detection System (IDS) monitors the data transfers and attempts to keep the WSN functioning by detecting malicious nodes in the forward path. This situation is modelled as a two-player, non-cooperative, zero-sum game

and it is proved that the game has no pure Nash Equilibria. This means that the game is unstable, and therefore does not provide a state at which we would expect it to be stabilised after a large number of iterations. In the resource-constraint environment of WSNs this instability is translated into increased power demands.

Kodialam and Lakshman [41] present a game-theoretic approach on detecting a network intrusion via sampling. Assuming that an accomplished malicious package transfer from an "entry node" to a "target node", as a result of a proper selection of communication paths, defines a successful intrusion, that every sample examination comes with a non-trivial cost and finally that in case a malicious packet is sampled then the intrusion is detected and circumvented, the authors tried to come up with a method that balances the antagonistic relationship between the intensification of the sampling and the cost restriction below the total available sampling budget. This was achieved by finding the Nash Equilibria of the corresponding two-player, zero-sum games and adopting the strategies that constitute them. The result was two heuristic algorithms for approaching the problem. The algorithms can be considered successful since their performance was proved upon some sample networks. In the positive characteristics of the model one could mention its applicability since it is applied in many real-life instances, however there is the not always true assumption that every malicious package is always detectable by the performed tests.

Another game-theoretic approach of an intrusion detection problem is the work of Tansu Alpcan and Tamer Basar [42]. In this work, the goal is the "development of a formal decision and control framework" with the use of two models. The first one is a simple to use and implement model that inserts different functioning modes to the Intrusion Detection System that will be adopted according to the warning level and uses concepts of cooperative game theory for the corresponding analysis. The second model is a more complicated one that presents the interaction between the attacker and the IDS as a two-player, finite game with dynamic information. As a result, with the use of those two models, the basic trade-offs of network security were addressed.

In [43], there is a game-theoretic approach where the case of multiple collaborating intruders attempt to inject malicious data into a target node and the defender (which in this case is represented by the IDS) tries to reject that attack. In this scenario, the group of intruders is handled like one single user and therefore a two-player, non-

cooperative zero-sum game occurs. In this game, the intruders in order to send their packages, always try to find the paths leading to the target node that will maximise the probability of successful delivery of the packages. The IDS on the other hand, can opt among different sampling strategies aiming to minimise the probability of a successful attack but also taking into account the underlying cost of each sampling strategy. Under that scheme, the authors demonstrate the optimal strategies that constitute the game's Nash Equilibrium.

In a similar fashion, the case investigated in [44] is a game-theoretic application of a resource allocation problem where the intruder sends malicious packets to the WSN from multiple entry points of the network while the defender seeks for the most efficient way to allocate the available recourses aiming in maximising the probability that the aforementioned packets are detected. According to the adopted deep packet inspection method, a subset of the incoming packets is selected and the corresponding packets are inspected. Unfortunately, this can lead to major delays in the throughput of the network. Thus, there is an upper bound for the fraction of inspected packets out of all incoming packets. The problem is again solved by making use of the notion of equilibrium and the optimal strategy of the defender, suggests the best options on where (inside the network) and how, inspections should be performed. A basic assumption that holds, once more, throughout the game is that once a malicious package is inspected, it is always detected and thwarted. Although the optimal strategies, as defined above, are found and validated experimentally in the project, it has to be mentioned that computational complexity leads to reduced scalability by rendering it intractable when applied on large networks. In order to overcome this problem, the authors came up with a polynomial approximation algorithm (called GRADE) which eliminates scalability problems, but they also introduce zero-sum simplified substitutes of the original networks when the latter are large.

The authors of [45] worked on a project that combined a game-theoretic approach and epidemiology in order to evaluate under what circumstances, it is beneficial for a network's operator to apply security measures and eliminate any security breaches the network may have. In a network, the security of every host is also affected by the security breaches of the other hosts of the network due to interconnectivity. Thus, the attack could spread in the network and the investigation of its behaviour requires the employment of epidemiology. In addition, due to the fact that every host is affected by the behaviour of

the remaining ones, a game-theoretic approach of a non-cooperative game was taken into account as well. Therefore, a unified framework that combines the SIS epidemic model that was employed in [46] with a non-cooperative game model was created. Since the protection from the breaches comes with a cost, bearing it may not always be the best choice, at least not for all hosts (which is possible since hosts decide autonomously). Indeed, the research proved that there are two thresholds for the cost of protection and when the actual cost surpasses the first one (which is constant), there is only one Nash Equilibrium which is achieved when all hosts are completely unprotected. On the other hand, if the protection costs less than the other threshold (which is a variable), every host should invest in it. Additionally, the authors provided a bound for the inefficiency due to the non-cooperation of the game and they noticed that in some cases it is excessively high. For these cases, they proposed two methods (by affecting the relative costs and by implementing an upper bound on infection probabilities) that could alter the network's equilibrium. Although it is a very interesting project that combines epidemiology and game theory there are two disadvantages that can be detected. Firstly, the fact that it is still unanswered what happens in case the actual cost is not greater than the first threshold and not less than the second (for the values of the second threshold that this is applicable) or in case the actual cost is both greater than the first threshold and less than the second. Secondly, it is a model that depends on the topology of the network and as such, it cannot be applied in networks with different topology.

In [47], the authors apply a game-theoretic approach on a WSN in an attempt to maximise the network's performance while compromising its power efficiency as less as possible and vice versa. In order for a WSN to keep servicing the purpose it was built for, the sensors that constitute it have to forward the information they receive from the other sensors until the information finally reaches the base station. Although, this goal will be served if some of the sensors stop forwarding incoming data, that will not hold if those 'selfish' sensors become more and more. The reason for which a sensor could not forward incoming information is power management, since every sensor spends non-trivial amount of energy when forwarding. To prevent a service failure both due to power insufficiency and vast amount of selfish sensors, the authors build a cooperative game-theoretic model based on reputation. According to that model, a reputation will be assigned to every sensor which will be designed in a way that selfish sensors will be

penalized so that they are motivated to participate in the forwarding procedure. In addition, sensors will be penalized when spending excessive amounts of energy. Another aim of the model is to isolate the most selfish sensors (i.e. the ones with the worst reputation) as this is an indication that they could be malicious. The solution to the problem will be the Nash Equilibrium of the whole game. The outcome of the model can be considered successful as the network could lower its power needs (in comparison to the WSN with a less sophisticated decision-making algorithm supporting it) while keeping its throughput in acceptable levels and the possibly malicious sensors isolated. The whole research could have great impact due to its many real-life applications and although the topology of the network is of crucial importance, which makes the model inapplicable in many cases, the authors have taken into account many different topologies and network properties.

In [48], the authors, focused on providing a precise and more efficient alternative to identifying the position of malicious nodes within a WSN than the existing methods that make use of GPS technology. Their method is based on modelling the interaction between the anchors (i.e.: sensors with known positions used in order for other sensors to determine their positions by multilateral triangulation) and the remaining nodes as a signaling game. The purpose of this work was not only the identification of when the secure localisation methods were required but also the optimisation of secure localisation costs by maintaining a low energy usage profile. In addition, the lifetime of the sensors would be substantially extended. This was different to what has been done in the past as the focus of the existing literature of such game-theoretic applications has mostly been within the context of Verifiable Multilateration trying to identify the best position of the verifiers in the WSN and increase the capability of localising malicious nodes securely by adopting a two-player non-cooperative game [49]; not on when it was required to activate a secure positioning method. The simulations conducted, proved that this mechanism is more efficient and only called when necessary (i.e.: when a node is classified as potentially malicious) than the one where secure localisation is always applied.

Authors of [50] proposed a hierarchical framework by adopting usage control (UCON) technologies and chance discovery, to improve the security of the WSNs by combining attack detection and prevention. UCON's dynamic attributes and continuous

decision-making, were used to mitigate the ongoing attacks in WSNs while a dynamic adaptive chance discovery mechanism was used to detect the unknown ones. At the same time, the low complexity and the high security requirements of WSNs were still taken into consideration. The aforementioned mechanisms were utilised by a unified framework in which low-level attacks were detected using simple rules applied on sensors and high-level attacks were detected using complex rules applied on the sinks and the base station. As far as the mitigation part is concerned, Software-Defined Networking (SDN) and Network Function Virtualisation (NFV) mechanisms were applied to that end, regardless of the type of the attacks. Finally, a simulation was conducted, for evaluating the attack detection and resource consumption rate and it showed that the proposed framework is feasible for WSNs and at the same time the detection rate, especially for unknown attacks, is higher than that of the most typical and existing detection schemes.

In [51], the authors proposed a game-theoretical framework by modelling a non-cooperative zero-sum attack-defense security game aiming to examine the interactions between an attacker and a defender within a cyberwar by dynamically choosing their strategies aiming to maximise their individual payoffs. In this model, each player has three possible strategies of attack/defense that are different to each other in terms of strategy cost, potential gain/damage caused and effectiveness in anticipating of the opponent's strategy. Finally, the authors find the mixed Nash Equilibrium of the aforementioned game and conclude that their method saves energy while attaining a high rate of success instead of having to have the defense system turned on constantly.

Elements of Originality

The content of this section is part of the answer to RQ1 by summarising the gaps of the existing literature on WSNs security and our addition to it. The actual additions consist part of the answer to RQ2, a more detailed response of which can be found in section 3.2.2, where our approach and its novelty are explained.

Compared to all those projects, our particular one can offer both a method that falls into the Intrusion Detection area and another that falls into the Intrusion Prevention one. Additionally, it combines some properties that are met in epidemiology models

which is something rear and only demonstrated once in the related work. Thirdly, the level of complexity found in our work can be considered significantly higher since there are demonstrated cases that two parameters affect each player's strategy simultaneously (which leads to multi-dimensional strategy sets), with a third one playing also its role although not being part of the strategy and that is something that renders the suggested models applicable to a much wider range of scenarios. Finally, our approach incorporates an iterated version that apart from its obvious interest due to the fact that it applies on situations where the non-iterated ones could not, it also gives the opportunity to perform forecasting based on this particular model's outcome. This idea will be further elaborated at the end of the project.

2.3.1.4 Game Theory and Epidemiology on Malware Dissemination Prevention

The way that viruses and worms spread in a computer network shares common characteristics with the proliferation of biological diseases in human populations. Therefore, the analysis of malware can benefit from investigating the behaviour of biological diseases. Two types of models for analysing malware proliferation in epidemiology exist, namely stochastic and deterministic models. Stochastic models (e.g., [52]) are used to analyse small-scale networks, and deterministic models are mainly used to analyse large- scale networks [53]. Our work focuses on malware spread in a large computer network, so we utilise deterministic models.

The majority of the deterministic epidemiology models are continuous-time models [54], since they offer higher precision when representing the emerging dynamics compared with discrete-time models. They divide the computer population of a network, known as *node population*, in discrete compartments, such as "Susceptible" and "Infected," and model the emerging dynamics between those compartments utilising differential equations. Individuals in the epidemic population may have several states, including susceptible, infected, and recovered. The differential equations used to model the transitions between those states form the mathematical description of each model.

Two models have been widely used in the field of epidemiology modelling: the SIR by [9][10][11] and a modified version of it, known as the SIS model [55]. Both models assume that all individuals within a closed population (i.e., no births and deaths)

are susceptible to the malware in the initial phase and an individual may go through each state sequentially. In the SIS model, the state transitions of an individual form a circulation. The individual may recover from the infection, but there is still a chance to be reinfected. In other words, an individual node becomes again susceptible to the malware after its recovery. In the SIR model, the final state is described as the recovered state. An infected individual can recover from the infection and become immune to the malware and an immunized individual cannot be reinfected by the same malware. However, neither SIR nor SIS can individually represent reality accurately; the SIR model lacks the option of returning an infected node into the susceptible pool, while the SIS model lacks the ability of immunization after recovery.

The authors of [56] proposed a modified version of the SIR model by introducing the notion of "temporary immunization." Their model (SIRS) consists of three compartments, Susceptible, Infected, and Temporarily Recovered. Individuals transit from the susceptible state to infected, from infected to temporary recovered and then back to susceptible. In reality this model introduces a delay in the traditional SIS model, since the infected individuals that recover return to the susceptible state after an amount of time. This amount of time is defined by the rate at which removals lose their immunization and become susceptible again. Resusceptibility represents the situation where a computer infected by malware recovers from the infection and becomes immune, remaining susceptible to modified versions of the same malware. Even though this model is more accurate than the traditional SIR and SIS models, it still lacks the ability to encompass situations where the individual becomes immune to the malware before getting infected. Furthermore, even though it takes into account the fact that a malware may appear in different versions, it does not clarify whether each version exploits the same vulnerability, in which case patching this vulnerability would immunize the computer against any variation of the same malware.

A similar approach is followed by [57], who proposed a dynamic discrete compartmental model. In their work, they mathematically formulated a four-state model encompassing the population compartments of Susceptible, Exposed, Infectious, and Susceptible with Vaccination (SEIS-V). This model adds one more state in the traditional SIS model, the Exposed state. By introducing this state, the authors denoted that not every susceptible individual is exposed. When a susceptible individual is exposed and comes in

contact with an infected node then he also gets infected. However, following the SIS paradigm an infected individual can recover and transit to the susceptible state. Another additional state is the Vaccinated state, where a susceptible node can be "vaccinated" and therefore immunized against a specific malware. Nevertheless, as in the work of [56], an immunized node can become susceptible again after a certain amount of time, and as before the authors do not take into account the mechanism of vulnerability patching. Furthermore, the exposed state is meaningless when modelling the spread of a random scanning malware in a fully connected network such as the Internet, where each individual within the susceptible population has the same probability of getting infected by an infectious node.

The focus in [58] is on modelling the spread of topological scanning malware. This type of malware spreads based on topology information. Therefore, the connectivity of each node plays a significant role in the malware propagation within the network, directly affecting the rate of infection. Unlike the previous model, it can also be used to model random scanning malware. Nevertheless, as mentioned by the authors, this model does not take into account patching and therefore there is no transition from susceptible to immunized.

Typically, disease spreading depends on common shared characteristics of the individuals in a population. In a network of computers, malware exploits certain vulnerabilities in the system in order to infect a host. [59] Common practice of malware is to exploit vulnerabilities in software that is installed in the victim-host. Thus, in order for a host to be considered as susceptible to a certain piece of malware, it must have installed the specific software version that bears the vulnerability that the malware can exploit. Otherwise, it cannot be infected and thus cannot be considered as susceptible. In the real world, not every host in a network carries the same vulnerabilities, forming therefore a heterogeneous computer network. This heterogeneity can be considered as an additional compartment of immune nodes. Our work has also taken into account the transition to this compartment from the susceptible or recovered state through the application of patching.

Authors of [60] took into consideration the dependability assessment of Heterogeneous Wireless Sensor Networks (HWSNs) with malware diffusion and examined their dependability and, with the aim of having a dependable HWSN, they

propose some metrics. In addition, in order for them to disclose the malware diffusion process, the authors proposed a heterogeneous discrete time SIS model that considers the heterogeneity of sensor nodes as well as the probability of malware choosing the Spread option (i.e.: self-diffuse) instead of Not-Spread. The aforementioned disclosure was achieved by the development of a non-cooperative, non-zero-sum game that formulated the relationship between a HWSN and the malware. During the whole process, a measure called Mean-Time-To-Infection (MTTI) had to be invented. Therefore, not only the infection behaviour of malware could be predicted but also the selection problem of optimal strategies for the purposes of balancing the costs and benefits of an HWSN system and malware could be solved. Consequently, a dependability assessment mechanism for HWSNs with malware diffusion, was set up.

In [61], the authors formulate a homogeneous WSN as a game where malware intelligently adapts its strategies in order to maximise the overall cost of the WSN while the system (could be the network operators) dynamically varies its strategies in an attempt to achieve the opposite. The developed model is based on epidemiology, differs a lot from the traditional SIS/SIR models and takes into account the sleep mode that the sensor may occasionally enter in order to save energy. With this procedure, the existence of a saddle-point which still meets the necessary Quality of Service (QoS) level and minimises the interference introduced due to the adoption of the corresponding security methods, is confirmed. The saddle-point strategies are able to limit the propagation of the malware and can be easily applied on the sensor nodes.

Elements of Originality

The content of this section is part of the answer to RQ1 by summarising the gaps of existing literature on CI-ICSs security and our addition on it. The actual additions consist part of the answer to RQ2, a more detailed response of which can be found in section 3.3.1.1, 3.3.1.2, 3.3.2, and 3.3.3.2 where our approach and its novelty are explained.

Our unified malware proliferation model, combines the traditional SIS and SIR while eliminating their omissions (as previously mentioned, SIR model lacks the option of returning an infected node into the susceptible pool, while the SIS model lacks the ability of immunization after recovery). This is done in a way that mitigates the aforementioned criticism about the existing work since providing patching capabilities allows the transition from susceptible to immunised. Finally, on top of that, it combines Game Theory to compute optimal strategies for the defender to minimize the effect of malware spread, while minimising the security cost.

2.3.2 Systems' Resilience and Optimisation

This section is about similar, or somewhat similar, literature applied on systems but this time from a perspective other than security. This section is, split in more categories that correspond to the categories of the following chapters. Specifically, there is a category about Game Theory applied on WSNs in order to somehow optimise the functionality of the latter and also another one about Hot-Desking.

2.3.2.1 Game Theory on WSNs Resilience

According to [62], the main categories that the game-theoretic approaches of such conflicts fall into are: Network Management, with indicative topics such as Resource Allocation, Task Scheduling and Power Control, Communication with topics like QoS, Topology Optimization and Routing Protocol Design, Network Security grappling with Intrusion/Denial of Service Attack Detection and Prevention and finally Applications such as Target Tracking, Data Collection and Packet Forwarding.

In terms of network management, communication and applications, [63] offers a model to improve the performance of a heterogeneous WSN, by taking into consideration the reliability, connectivity and the power efficiency of the network. The results indicate that the existence of a Nash Equilibrium is always achievable. In similar work, [64] builds an energy-efficient control model, which offers great improvement to energy reduction in terms of QoS. it attempts to improve the so-called Gur Game algorithm [65], a mathematical model that is used for self-control in cooperative environments.

Authors of [66] propose a Localised Game-theoretical Clustering Algorithm (LGCA), which tackles the problem of choosing the most appropriate Cluster-Heads. It attempts to improve the Clustered ROuting for Selfish Sensors (CROSS) [67], and the Low-Energy Adaptive Clustering Hierarchy (LEACH) [68]. As the most fundamental part of the proposed solution, knowledge on the number of players (nodes) in each round is considered unnecessary. The key for this is that each node plays a clustering game only with its neighbours within a predefined radius. Moreover, exactly one node can bid for a position of the Cluster-Head in one district successfully, in order to achieve an optimal payoff. Simulation showed that LGCA performs better than CROSS and LEACH in terms of network lifetime. Focusing on security related applications of game theory within WSNs, [40] investigates cases where a clustered WSN is under attack. The proposed IDS monitors the data transfers and strains to keep the WSN functioning properly. This situation is modelled as a two-player, non-cooperative, zero-sum game where the attacker's reward is proportional to the damage caused to the network and the defender, which is represented by the IDS, receives a reward proportional to the network's functionality. As a result, it is proved that the game has no pure Nash Equilibrium.

In [39] a reputation system on different sensors is applied in order to make it more energy efficient and secure. Forwarding packages, in a fashion required by both ends, brings positive reputation to a sensor, but also consumes more energy, which could ultimately affect the networks performance later. There are malicious nodes that are injected in the network in order to randomly drop packets in order to shut down nodes with low reputation. In such cases there arises a number of conflicting motivations, where game-theoretic tools could offer a suitable solution. This model, which extends the works done in [69][70], attempts to divide nodes' interaction into three distinctive domains including: any node-to-node communication, one-hop neighbours communication and inner-cluster communication. It concludes that for all three types, there can always be a Nash Equilibrium, by which security and power conservation can be improved.

In [66] there is a game-theoretic approach of multiple collaborating intruders who try to inject malicious data into a target node and the "defender" (the IDS) tries to prevent the attack. Since intruders can be assumed to act as one, there is a two-player, non-cooperative zero-sum game that occurs. Intruders, in their attempt to send their package try to find the paths leading to the target node that will maximise the probability of

successful delivery. The IDS on the other hand, can opt among different sampling strategies aiming to minimise the probability of a successful attack always by taking into account the underlying cost of each sampling strategy. Under that scheme, the authors demonstrate the existence of a Nash Equilibrium and the optimal strategies.

Authors of [71] worked on a game-theoretic clustering algorithm that is applied on WSNs and its scope is to improve the network's load balancing, as well as its execution time and energy consumption. The algorithm attempts to decide which node(s) will act as Cluster-Heads and which not. It is based on the principle that all nodes are 'selfish', meaning that they would all prefer not to be Cluster-Heads. However, if there is no Cluster-Head in the network that would lead to all of them not gaining any utility. Therefore, that leads to an antagonistic situation where, on one hand, nodes would prefer to not act as Cluster-Heads but, on the other hand, there has to be at least one Cluster-Head in the network in order for the nodes to be able to gain some utility. That makes Game Theory a suitable tool for the solution of this problem. The proposed algorithm is compared to Chor Ping Low's approximation algorithm (GLBCA) [72] and Gaurav Gupta's algorithm LBC [73] and is found to outperform both of them in terms of load balancing[3], execution time and energy consumption.

The work of Duan Jungi et al [74] is also about improving efficiency of the trust evaluation process in WSNs. In particular, the authors introduce a custom energy-aware trust derivation scheme which aims to keep the consumed energy and the latency of a WSN at a minimum, while at the same time maintains its security at an adequate level. To that end, they firstly present a method of risk strategy analysis that stimulates cooperation among the nodes of the WSN and secondly, they introduce a game-theoretic approach, the so-called Trust Derivation Dilemma Game (TDDG) in order to reduce the overhead of the network. The TDDG is based on the principle of the nodes being evaluated by their neighbouring ones. Each participating node can choose between Reply and Not Reply when receiving a trust request by another node. There is also a mechanism that prevents nodes from their default inclination to not replying, in order to preserve battery. The network is considered secure only if the number of recommendations is

[3] In order to judge the quality of the load balancing, we measure the standard deviation of the loads of the CHs and plot against the number of sensor nodes.

greater than a specified threshold. Finally, the numerous simulations that are made lead to the result that this whole approach is not only able to keep the security levels of the WSN at the desired level and reduce its energy consumption when compared to traditional mechanisms but also to do it with only a minimal increase in latency.

The authors of [75], presented a decentralized, scalable and stable 3D game-theoretic energy balance (3D-GTEB) routing protocol, which manages to improve the routing decisions while minimising the network overhead and at the same time improving the energy balance (by attempting to lead to the energy of all the sensor nodes getting depleted approximately at the same time), using two levels of decision making. The first level, which is called wedge level energy balance, balances traffic load over a set of forwarding wedges using evolutionary game theory. According to the authors, the latter can demonstrate significant improvement in the lifetime of the network and also in energy consumption per packet. The second level is called node level energy balance. This technique captures the infamous selfish nodes' behaviour of not participating in forwarding in order to preserve their energy and encourages them to participate in forwarding, by using classical Game Theory. The simulation conducted, proved that the proposed routing protocol can improve and extend network's lifetime compared to a 2D-GTEB (Two Dimensional Game-Theoretic Energy Balance).

Elements of Originality

Differently to the existing work in this field, we combine Game Theory with SensomaX, a custom agent-based WSN middleware developed by Dr. Mo Haghighi. The many benefits of this approach are mentioned later in the corresponding chapter, where it is more appropriate.

2.3.2.2 Hot-Desking

The key value driver of the initial applications of Hot-Desking was that office sizes could be reduced up to 30%[4] depending on the tendency of the business to visit clients and collaborators outside the premises.

Today, the most common form of Hot-Desking is simply "employee-led" (i.e.: on attendance to the office, an employee chooses a desk themselves that they deem to be unoccupied and claims it for the day).

While the value case presented by Hot-Desking is summarized as being relatively clear and by no means insignificant, such schemes have had mixed success [76]. Today's literature's criticisms can be broadly categorised into the following key aspects:

- Ineffective management: A mixture of slow and inconsistent methods of distributing desks, ranging from "this desk is free" signs to entirely free-for-all situations, introduces misunderstandings about whether or not a desk is occupied [77].
- Loss of working synergies: In traditional territorial (i.e. "assigned") working systems, members of a specific teams are assigned desks in close proximity to one another to enable easy and regular collaboration and discussion between individuals working on similar projects and on similar themes. When desks are assigned either randomly or linearly in a "pegs into a slot" system, this is lost. While it is difficult to attribute the impact of this on issues, such as productivity and employee happiness, it could be envisaged that even small variations (e.g. 1% decrease in productivity) have significant impact on even the smallest scales [78].
- Cultural and behavioural barriers: A territorial working system encourages individuals to build and adapt their desk to their own personal preferences and working ideals; with a Hot-Desking system, these are lost. This ranges from sentimental issues, such as photos of loved ones and favourite literature, to working documentation, such as large drawings and annotated reports, to

[4] "BBC iWonder - Is hot desking all good?" [Online]. Available: http://www.bbc.co.uk/guides/zgjmtfr

office furniture, such as specific ergonomic desk heights and chair configurations [79]

It is clear that there are significant shortcomings to the use of Hot-Desking within a commercial office environment, which can be broadly translated to influence on employee productivity. There is a consensus that these benefits in general are inherently hard to quantify.

The rise of data collection and connectivity as detailed in the introduction can be hypothesized as an opportunity to fundamentally alter the nature of Hot-Desking by utilising increased data about the workplace, its occupants and their intentions and preferences. While this is theoretically possible, little research exists on how optimization might look in practice, and on the value it could bring to the workplace. What does exist however is considerable discussion of the workplace and its influence on the occupants.

Although there are quite a few definitions of "productivity", a rather general one, that we can also adopt for the needs of this work, is the one of [80], which is "the ability of people to enhance their work output through increases in the quantity and/or quality of the product or service they deliver". According to [81], health and well-being are two "prime requisites" of productivity, where health is an employee's mental and physical health and well-being is the perception of the employee of their satisfaction and happiness. Because health and well-being are inextricably connected to productivity, a configuration that manages to improve either or both, is a means of increasing productivity.

A framework for the measurement of office productivity using factor analysis has been formulated by [82]. The components were initially seven but were refined by the author to four, which are listed in Table 2.

Table 2: The four components of office productivity according to [83]

Category	Component	Variables
Physical Environment	Office Layout	Work area, overall office layout, meeting areas, quiet and/or private areas, personal and general storage, circulation space
	Comfort	Ventilation, heating, lighting, decoration, cleanliness, physical security
Behavioural Environment	Interaction	Social / work interaction, creative physical environment, overall atmosphere, position relative to colleagues and/or equipment, overall office layout
	Distraction	Interruptions, crowding, noise

The decision-making process of a Hot-Desking model could take many of these variables into account. These could be some of the following, which correspond to elements of Table 2:

1) Nature of work [83]. Not all employees of a company work on the same project or even the same theme of project. Therefore, each employee's office attendance could be associated with specific projects or skills, and a distribution system could try to put employees that work on the same project, or using similar skills, close to each other, which could be theorised to make them communicate better and thus be more productive. Indeed, interviews undertaken in support of this paper suggest, this "proximity synergy" may even be better than traditional allocated systems because desk associations are typically totally re-evaluated on anything from a yearly to 10-yearly basis and also because an intelligent system allows people to vary their associated group on a day-to-day basis. In general, this is only currently done on extremely

large “megaprojects”, such as the London 2020 Olympics, but evidence suggests these create powerful working environments; there is a suggestion that, if it could be made practical, then similar benefits would be realised for such groupings for smaller and part-time projects.

2) Noise level [84]. Noise levels and the distractions that these can cause have a significant impact on the actual productivity [85]. Therefore, it is important to put employees with similar needs. For example, attention-to-detail work usually requires quiet environments and typically generates little noise, whereas team-focused work may not necessarily need a loud environment, but will be able to function in one, and will certainly contribute to the noise. Data for noise levels can be derived from acoustic sensors distributed about the office or estimated from input data on employee’s principle tasks for the day.
3) Duration of stay in office. This information could be derived from calendar data or asked for upon arrival. Individual’s staying for exceptionally short periods of time is probable to be happy with smaller and more casual “touch down desk”. This may further improve the floor area savings of traditional Hot-Desking.
4) Environmental preferences [86]. This information could be derived from many types of data set, including temperature and light sensors across the office. Many small miscellaneous factors have been identified as being significant in the workplace, and achievement of these could be improved by consideration of individual’s preferences. For example, individuals who prefer a warmer office environment could be placed further away from colder areas, typically atriums and stairwells.

With the rapid growth of Smart Building technology, some of the variables of Table 2 are easy to be monitored and changed automatically, especially the ones that correspond to the component of comfort. For example, studies show that improving lightning conditions can improve productivity even up to 20% in some cases [87], while proper air quality has been found to improve productivity by 6%-9% [88]. Furthermore, improper heating can decrease productivity by about 10% [89], while the ideal office

temperature has been found to be between 22 and 26°C [90] although the regulations differ by country.

This is possible because there are already many affordable commercial solutions available for collecting data to inform these parameters. However, when it comes to commercial solutions for the distribution aspect, using these data sets in a way that will aim at a productivity increase, there are no products or services observed in the market. Despite the absence of literature covering the possibility of digital innovation in hot-desking, the aforementioned specific areas, combined with the corresponding hypotheses, form possibilities for an optimisation use case to assess the value proposition and practicalities of an intelligent Hot-Desking implementation. As it is described below, this model will take into account the "nature of work" variable.

The literature that is related to Hot-Desking can be mostly categorised into three main research topics. Firstly, it is the topic about the impact of Hot-Desking on the health status of the employees. The second category is related to the examination of the evolution of the workspaces throughout the years. Finally, the third one is about the importance of the workplace for the employees and its impact on their productivity or even on the mind-set and their sense of team spirit. Existing studies were not found to have similarities to this one. Related work that is presented here is about different use cases that the concept of Hot-Desking is used for and although they can be seen as somewhat similar to our work (by various criteria that are explained below) they are still remote enough.

It is worth mentioning that the definition of Hot-Desking is somewhat vague and therefore some conflicts can often occur among different authors [91][92]. However, the term 'hot desks' is most commonly used in order to express 'desks that can be used each time by a different user' and this is the definition that we will use in this work.

It is often due to this controversy on the definition, that the topic of Hot-Desking is related to Sit-and-Stand desks and therefore to employees' health. Authors of [93] for example relate hot desks with standing desks and they look into the impact that this kind of desks has on the sedentary work time in an open plan office. According to the findings, these desks did not have a great impact on the sitting working time of the employees.

In a similar fashion, the effectiveness of sit-stand workstations in terms of their ability to reduce employees' sitting time is studied in [94]. However, the findings from

this ‘Stand@Work randomised controlled trial pilot’ differ significantly from the previous one since that study shows that these kinds of desks can indeed reduce sedentary work times in the short term. It should be mentioned though that authors note the necessity of larger scale studies on more representative samples in order for the exact impact of sit-stand workstations on the health of individuals to be more accurately determined.

In [95], an attempt for results of six related pieces of research to be compared is made. All six of them are about the effect that some interventions at the workplace can have on the sitting habits of the employees during their working hours. The interventions vary from one another and in all of them, sitting time had not a significant decrease due to the aforementioned interventions.

Authors of [96] relate hot desks with sit-stand desks. These are desks that are considered ‘hot’ according to the definition that we adopt, with the specificity of being used in a standing position. The objective here was to examine whether the use of these desks along with awareness regarding the importance of postural variation and breaks would manage to cause better sedentary habits for the employees. The results showed that the adoption of these desks led to a better sedentary behaviour.

In a fashion similar to the previous works that were presented, authors of [97] experiment on the effect that the installation of sit-stand workstations could have on the reduction of worker’s sitting times. In this study the results were very encouraging since the adoption of the sit-stand workstations was astonishing with huge impact on the sitting times (‘Sitting was almost exclusively replaced by standing’). However, although the strong acceptability of these workstations, there were some design limitations that should be considered in future attempts.

All the aforementioned pieces of research belong to the first of the three categories that the bibliography can be summed up to (i.e. the impact of Hot-Desking on the health status of the employees). Below, we present characteristic representatives of the remaining two categories. Representatives of the second category (i.e. examination of the evolution of the workspaces throughout the years) followed by the ones related to the importance of the workplace and its impact on the productivity, mind-set and team spirit of the employees, which is the third category.

The evolution of the workplaces is examined at [91]. In particular, its authors investigate the rate of adoption of modern-type workplaces, including but not limited to

Hot- Desking. It is interesting though that the authors define 'hot desks' as 'desks which workers have to book in advance to use' while the definition we adopted resembles more the definition that authors use for 'collective office' which according to them is 'facilities that are shared and used on an as needed basis'. Combining many sources of evidence, authors conclude that although workplaces tend to differ more and more from the typical conventional ones that were used in the past almost exclusively, this is happening with a slower rate than some claim. The findings of this study are mostly confirmed by the findings of [79]. According to the evidence of the latter, office work is increasingly differentiated from the traditional workplaces although for the majority of employees, work still corresponds to a designated place.

In [98] we meet once more the concept of Stand@Work, but this time it is not its impact to the sedentary patterns that is investigated. Instead, the objective was to qualitatively evaluate the willingness of the employees to adopt new types of workplaces, the feasibility of such a venture and the general perception of employees about the use of sit-stand workstations. The whole scheme was generally perceived as both acceptable and feasible although studies with different populations and settings need to be made.

Another study [98], considers Hot-Desking within the grand scheme regarding the societal changes in the ownership of space. The aim of this study is to sociologically analyse the emergent sociospatial structures in a Hot-Desking environment where space is used by more than one users, exchangeably. The study results in two interesting findings. Firstly, the find that the perception of mobility may not be spread evenly among the employees, resulting in two different groups of them: the settlers (i.e. the most resistive to change) and the 'hot-deskers'. Secondly, according to the findings, the routine of mobility itself can generate additional work and a motion of marginalisation to the adopters.

For the third and final category of related studies, we can include [76] as well, although it belongs to the previous category too. That is because its findings are related not only to the evolution of workplaces but also to the impact that this has on the adopters, from multiple perspectives.

Apart from that study, there is also [78] which examines the impact of Hot-Desking on organisational and team identification. The study tested the level up to which the organisational and the team identity are affected by the way desks are assigned and

secondly the impact that physical arrangements have on the level of engagement with the organisation. According to the results, team identity is more salient than organisational identity when a traditional desks assignment is applied whereas organisational identity is more salient when Hot-Desking is applied. The findings also denote that physical arrangements not only have significant impact on the level of engagement of the employees, but also on the on the type and focus of organisational participation.

Elements of Originality

The content of this section is part of the answer to RQ1 by summarising the gaps of existing literature on Hot-Desking and our addition to it. The actual additions consist part of the answer to RQ3, a more thorough response of which can be found in section 4.3.2 where our approach and its novelty are explained.

It is obvious from the related work that is presented, that research in the field is relatively undeveloped, especially when we consider when existing studies were made. Most importantly though, there is a big gap in the bibliography when it comes to the research of the connection between the Hot-Desking and the productivity of the adopters. As shown already, studies on that connection are very scarce and even then, it is only an indirect connection that researchers usually study. Now, researchers almost always examine the implications of Hot-Desking on health, or more specifically on the sedentary habits of the adopters. Even the impact on profitability (which is one of the reasons that Hot-Desking was initially developed as it leads to reduced desks and resources in general) has been ignored by the aforementioned approaches.

Furthermore, the nature of the existing work is such that no modelling is performed in order to utilise Hot-Desking in the best possible way, both in terms of organisation's profitability and employees' productivity. Thus, we could say that existing literature has not managed to keep up with the needs of modern business environments.

What we offer is a different view; a model that based on occupancy data of the employees, calculates and suggests in real time which desk to be assigned to every employee at the time they arrive at the organisation. The model decides which desk will make the incoming employee or all the employees as productive as possible, based on the

project that they are working on, at that period of time. That way, not only employees find themselves working in the most productive environment possible, without having to decide the sitting arrangements themselves (with any disadvantages that this would entail in terms of the relationships among them) but also the organisation will have a double benefit as it will make profit not only due to the number of desks that will not need to be used anymore (desks will be less than the employees while still covering their needs), but also due to the fact that all employees will work under optimal productivity conditions.

To the best of our knowledge, there is no similar approach published.

II. RESEARCH CONTRIBUTION

Section II, includes Chapter 3 and 4 which consist of our proposed models. In particular, the former includes the security and risk management-oriented part of the research with models on the security of WSNs and four different use cases on the security of CI-ICSs while the latter includes models on the resilience of WSNs and Hot-Desking.

Chapter 3

SYSTEMS SECURITY AND RISK MANAGEMENT

Chapter 3 discusses the common systems-related issues and provides some use-cases applying the proposed models on improving WSNs and CI-ICSs from a security and risk management perspective, along with the research findings. Within this chapter, RQ2 is addressed.

This chapter includes material from the following published papers, as per below:

Section	Published paper
3.3	Maraslis, K., Spyridopoulos, T., Oikonomou, G., Tryfonas, T., & Haghighi, M. (2015). Application of a game-theoretic approach in smart sensor data trustworthiness problems. In IFIP International Information Security Conference (pp. 601–615). Springer.
3.3.1.1	Spyridopoulos, T., Maraslis, K., Tryfonas, T., Oikonomou, G., & Li, S. (2014). Managing cyber security risks in industrial control systems with game theory and viable system modelling. In 2014 9th International Conference on System of Systems Engineering (SOSE) (pp. 266–271).
3.3.1.2	Spyridopoulos, T., Maraslis, K., Tryfonas, T., & Oikonomou, G. (2017). Critical infrastructure cyber-security risk management. Terrorists' Use of the Internet: Assessment and Response, 136, 59
3.3.2	Fagade, T., Maraslis, K., & Tryfonas, T. (2017). Towards effective cybersecurity resource allocation: the Monte Carlo predictive modelling approach. International Journal of Critical Infrastructures, 13(2–3), 152–167.
3.3.3	Spyridopoulos, T., Maraslis, K., Mylonas, A., Tryfonas, T., & Oikonomou, G. (2015). A game-theoretical method for cost-benefit analysis of malware dissemination prevention. Information Security Journal: A Global Perspective, 24(4–6), 164–176.

3. SYSTEMS SECURITY AND RISK MANAGEMENT

This chapter will focus on examining common systems-related issues from the perspective of their security and risk management (as opposed to the next chapter that will examine issues from the perspective of their utility and resilience) following novel methods. Overall, the chapter investigates some use-cases which can be divided in two general categories: the ones related to WSNs and those that are related to CIs and ICSs (without implying that a system cannot fall into both of these categories).

3.1 Introduction

Systems' security and risk management techniques have plenty of space for improvement. To this end, in the following sections we present some use cases where we apply methods with explicit benefits (that are described in the corresponding sections) compared to the more conventional existing ones. As discussed before, the cases explained fall into two main categories; WSNs and CI-ICSs with the latter one including, among others, a use case where Monte Carlo predictive modelling is applied and another one using Epidemiology. Although, these two are used within a context that is not explicitly presented as CI-ICS, they can both easily fall within the definition of ICS, no matter which of the two most dominant ones [17][99] someone chooses to adopt; not to mention the vaguer definition of CI.

3.2 Wireless Sensor Networks

Wireless Sensor Networks constitute a very important and often critical field with a great amount of research around it. In the following section there is some background knowledge on WSNs, the proposed models for an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) which are followed by a double validation of their results, one in a cluster-based deployment and another one in an IPv6 one.

3.2.1 Introduction and Background Knowledge on WSNs

The use and progress of the WSNs, especially the recent years, has been dramatically increased since they can now offer a low-cost solution to the challenges of today's world [100][101]. WSNs are homogeneous application-centric networks comprising of several autonomous devices (sensors) that are spaced accordingly in the network [102][103], measuring environmental or physical conditions like temperature or pressure [104], working together to collect necessary data, and sending them through the wireless network to the final central position [102][103]. They are used in numerous instances with great advantages for the quality of life of millions of people every day [100]. However, those networks come with their vulnerabilities. Those vulnerabilities can be used by intruders in order for them to cause damage to the data or the network itself. Therefore, the field of Wireless Sensors Network Security is critical since it investigates ways that those intruders can be mitigated, and data can be communicated and used safely and efficiently.

Two vigorous areas of Wireless Sensor Network Security field are the IDSs and the IPSs. The former area is about methods that can enable the network operator to detect an intrusion to the network while the latter expands the potentials and introduces the probability for the operator to block the intrusion. One can easily surmise the huge importance of such systems if they think of the potential damage that an intrusion can cause, from every possible aspect. In this chapter, there are two models that are demonstrated. One that falls into the general category of Intrusion Detection Systems (or algorithms) and another one that can be seen as an Intrusion Detection System (or algorithm).

Problem Definition and Scope

In the models studied below, there is a WSN along with an attacker (who will be assumed female from now on, for better understanding of the work in some cases) and a defender (who will be assumed male from now on, for the same reason) of this network. The former can attack the WSN using some or all of her resources while the latter, who can be assumed to be the network operator, can defend the network using again some or

all of his resources. The problem is that the more of their resources they use, the more cost they incur and the more profit at the same time. Since it is not obvious what part of their resources both parts should use in order for them to have the highest possible profit for themselves and taking into account that the more profit one has the less has the other, there is a complex problem that arises that makes a Game-theoretic approach suitable since adversarial strategies are involved. This is, roughly, the problem that will be analysed and solved.

The use case that the first model is applied on is a WSN that measures a characteristic (e.g. the temperature) of a predefined area. According to this use case, the attacker tries to compromise the network by making the sensors transmitting faulty measurements instead of the real ones. The scope of the introduced algorithm is to enable the defender (e.g. network operator) to adjust the network parameters he can affect, before an intrusion is attempted, in the best possible way so that that the least possible faulty information is used when the attack occurs.

The second model applies on the same use case, but it now offers an intrusion prevention mechanism as well. It can be used as a tool to prevent an intrusion or at least reduce the impact as much as possible. Its scope is to enable the network operators to adjust the network parameters they can affect, in a way that the damage of the infiltration can be minimised in the best possible way.

Detailed descriptions of the methods used, and the parameters mentioned are given later in the chapter where the whole analysis takes place.

Basic Information

Some useful basic information and essential notions of the involved technologies are presented in this section for a better understanding of the analysis that follows later and understanding of the wide use, and therefore importance, of WSNs.

A WSN, is composed by self-powered sensors (or nodes; these terms are used interchangeably in this thesis) bounded from a small number to thousands [105]. Depending on the case, each of these sensors is linked to one or more others [100]. When there is no possibility of using cabled sensors, the use of a WSN offers consistency,

reliability and low power. Energy, storage, processing power and communicational characteristics are some of the limitations of each sensor network node.

A self-powered sensor is divided into the following parts: a microcontroller, a transceiver which may have an internal antenna or work in conjunction with an external one, a possible interconnection of the sensors with an electronic circuit, a memory unit and a source of power (battery in our case). The size of each node is not always the same even within the same network and its cost can vary a lot depending on its characteristics. Often, constraints on size and cost cause additional restrictions on resources such as energy, bandwidth and memory [100]. The topology of WSNs varies from a simple star network to a more advanced multi-hop wireless mesh network Routing or flooding may be the spread method between the network hops. The figures below, illustrate a characteristic simple star network and a multi-hop WSN.

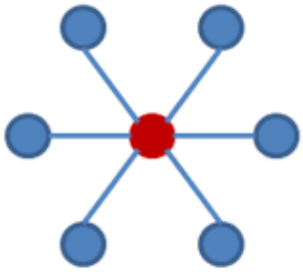


Figure 3: Characteristic Simple Star Network

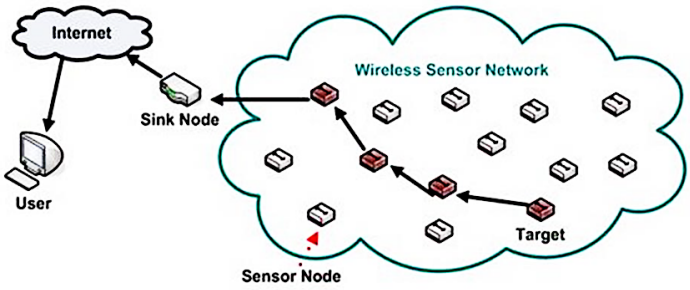


Figure 4: Characteristic multi-hop wireless sensor network [106]

WSNs have many applications and among others, they are used widely in transportation, security, science and civil infrastructure [44]. Some interesting examples

WSNs have many applications and among others, they are used widely in transportation, security, science and civil infrastructure [44]. Some interesting examples are surveillance, child education, machine health monitoring, environmental monitoring, micro-surgery and monitoring or studying natural phenomena (e.g. hurricanes, forest fires) [102][103][105]. Military applications like battlefield monitoring caused the expansion of WSNs [102][103][107]. A continuous tracking of an object, human or characteristic is detected in most of the monitoring applications.

Security in Wireless Sensor Networks

The possible vulnerability of a WSN to attacks, causes the necessity for security measures. The major reason for that is the wireless nature of the network since physical access of the attacker is not necessary [108]. Security in WSNs is essential for guarding safety and privacy of sensitive data [109]. The main difficulty in network security is the nature of decision making. Protection strategies are used by nodes and network users in order to overcome security vulnerabilities. When users and nodes are taking autonomous decisions then a non-cooperative game is raised due to the fact that these decisions affect other users [45]. False information could be sent from malicious nodes to other nodes in the network or private data could be intercepted. These phenomena occur due to the absence of security in a network [110].

There are many reasons for which security in WSNs is complex. Firstly, wireless communications used by the sensors are easier to eavesdrop. Secondly, WSNs are not always secured physically and sometimes they can be located in an unsafe environment. Furthermore, for a network with many sensors, it would be difficult to defend each one from a natural disaster. The instability of a WSN is caused by a large number of different security threats that are invented by the attackers. Therefore, what is required is, firstly, data confidentiality which is the main subject in the network security. Secondly, data integrity, the property that ensures that received data is delivered unchanged and finally, availability which is the last among the most important security requirements. Although these three are the main requirements of the data security, authentication, data freshness, self-organization, time synchronization and secure localisation can also be considered for the list [101][104].

IDSs expand the standard of information security across traditional protective and reactive security. IDSs can monitor or even control WSNs and are crucial in detecting attacks in the latter and reinforce the growth of IPSs [42]. Monitoring and controlling the network, gives the opportunity to the administrator to react against many possible security issues. When attackers damage nodes or network resources or alter their behaviour, then this is considered an intrusion. IDSs are responsible to alarm outright when an attack is detected so that the operators can prepare their actions [101][111]. IDSs are usually categorised into rule based (or signature based) IDSs and anomaly-based ones. Although, rule based IDSs, detect accurately the well-known attacks since they have predefined rules for them, they are incapable of detecting new attacks where the signatures are not included in their database. On the other hand, anomaly based IDSs can detect new attacks apart from the well-known ones by monitoring traffic patterns or the utilization of resources [111][112].

IPSs attempt to prevent attacks from entering the system or making the impact of the attack as mild as possible. IPSs that cooperate with an IDS or include such a mechanism, can be called Intrusion Detection and Prevention System (IDPS) [113][114]. IPSs mostly use one of the following detection ways. Rule Based (or signature based), Anomaly Based or Protocol Analysis (comparison between observed activity and predetermined profiles of actions that are considered non-malicious) [115].

Having presented the very basics on the security of WSNs, IDSs and IPSs, it has to be pointed out that in order for the defender to decide how to react against the detected attacks, a decision-making framework is essential. Game Theory has been proved to be a powerful scientific tool that could be used for analysing and modelling the decision-making procedure in situations where antagonistic interests take place, such as an attack against a WSN where the attacker and the defender have, obviously, adversarial benefits. Therefore, Game Theory has gained much interest over the last years for cases like these [42][116][117].

3.2.2 Proposed Models and Case Studies on WSNs

The content of this section addresses part of RQ2 by demonstrating how Game Theory can be used in order to build an IDS and an IPS that are applied on a WSN in order to enhance its security.

As already mentioned, IDSs and IPSs are two fields of significant research development. In this section, the presentation of two models takes place, one for each of these categories. Firstly, there is an IDS and afterwards, two versions of an IPS, an iterated and a non-iterated one.

3.2.2.1 Intrusion Detection System

In this model, a game between the defender which could be the security team responsible for the seamless operation of a WSN that gathers data about the temperature of the area under monitoring and the attacker who randomly chooses which sensors to attack and tries to make the network transmit as much incorrect information as possible, is replicated. It should be noted that in this scenario, a compromised sensor cannot affect the other sensors in any way. Even if it needs to forward packages of an uncompromised sensor towards the base station, it is not possible to distort them before sending. Thus, considering that some sensors are attacked, all the remaining sensors, including the neighboring ones, will keep functioning properly, which is a realistic assumption.

As in any game in strategic form, the players (attacker and defender in this case) have their adversarial strategies and the parameters that define them. Any possible combination of those generates a payoff for each of them. This particular game can be considered a two-player zero-sum one which means that only one player's payoffs need to be specified since the other player's payoffs will be the opposite ones. In addition, it is assumed to be a static, non-cooperative game, properties that were chosen due to their realism and applicability on the model.

Since the defender needs to monitor a specific, predefined area, sensors have to be spread throughout the area of interest. The question that naturally rises is what the

density should be (i.e. number of sensors per area unit) that the defender should choose. Since the region under investigation is predefined, it is only the **number of sensors** that can affect this density. Hence, the number of sensors is part of the strategy of the defender and throughout the game the player should try to find the most beneficial number within a set of realistic choices.

In addition, there is a **significance coefficient** for every sensor. This coefficient is proportional to the level of trust that is related to the information transmitted by this particular sensor. In other words, it reflects the trustworthiness that the network operators assign to every sensor and in a way, echoes the probability that the measurements provided by the sensor are indeed true. The reasons that this coefficient differs from sensor to sensor could be various. Firstly, it is depended on the kind of measurements that are taken. If, for example, it is the temperature under measurement, as in this case, then the spot that a sensor is placed on can affect the measurements. If the network is already set and has, even a small, history then those coefficients could be the outcome of an ongoing learning procedure and therefore reflect how trustworthy were the past measurements of each sensor. It is also worth mentioning that two sensors with identical specifications, operating within the same area can still report slightly different values due to structural features of the sensing elements. Although significance coefficients can affect the game, they are not something that the players can choose or change so they are not part of anyone's strategy.

Apart from this parameter, **tolerance** is also part of the defender's strategy and it is a property of the whole network. Having defined **untrusted / trusted / total information** as the sum of significance coefficients of untrusted / trusted / all sensors, respectively, tolerance denotes the minimum portion of the total information that the untrusted information should be, in order for the latter to be believed by the defender. In other words, it denotes the minimum value that the following fraction can have in order for the incorrect information that has been injected into the network to be treated as correct. We call this fraction Attack Coefficient (AC):

$$Attack\ Coefficient\ (AC) = \frac{Untrusted\ Information}{Total\ Information} \qquad (6)$$

This is part of the defender's strategy since he is the one to decide which piece of information is treated as valid. The choice of tolerance can directly affect players' tactics due to formula (7) that we will see later on.

Before AC can be of some use, some further aspects regarding the attacker's behaviour need to be clarified. It is realistic to assume that the sensors, under normal circumstances and when they are not under attack, transmit information that although it can be slightly different from sensor to sensor, it does not change dramatically since all sensors measure the same characteristic of the same area. Thus, in order for an attack to have a point and a possibility of success as great as possible, it is realistic to assume that the attacker's goal is to make a sensor transmit data that demonstrates noteworthy deviation from the data that uncompromised sensors transmit and at the same time, all compromised sensors transmit (erroneous) values that are very close to each other.

At this point it is essential that some basic assumptions of the model are presented:

1) Players are rational (i.e. they want to maximise their individual reward and they are considered risk-averse).
2) Full area coverage is desired.
3) Two sensors of the same network with identical specifications, operating under identical conditions can still report slightly different values.
4) A compromised sensor cannot affect the information that other sensors transmit.
5) The attacker's goal is to make sensors transmit faulty values that demonstrate noteworthy deviation from the ones that uncompromised sensors transmit but still (faulty) values similar to each other (for the reasons explained before). Additionally, the attacker only affects the information transmitted and not the protocol itself.
6) Compromised network is the network into which the injected faulty information is believed by the defender.

Under those assumptions, the network operators try to take into account only the non-compromised data without knowing in advance which piece of data is compromised.

Therefore, if the attack coefficient is greater than tolerance then the incorrect information is considered to be accurate, correct data is disposed and the attempt for compromising the network is considered successful, which in turn increases attacker's payoff. Otherwise, the network is not considered compromised, which implies a lower payoff for the attacker. Thus, the algorithm and, in turn, the defender can judge whether the network is under attack by the percentage of the believed information out of the total information which justifies its inclusion in the IDS category. Intuitively, tolerance should only be a value greater than 0.5 (50%) and of course less or equal to 1 (100%). In this way, the weighted information that will be ultimately "believed" by the defender will correspond to at least half of the total weight. Our goal is to help the defender choose the best options (i.e. options that will lead to the highest possible payoff for him) about the number of sensors that will constitute the network and the tolerance adopted.

Since the only aspect that the attacker can affect is the number of sensors to attack, she will have to choose the most beneficial number of attacks within a set of realistic values for this purpose. Of course, every attack comes with a cost as is the case for the sensors, each of which comes with an obtaining and maybe installation cost. Therefore, it is not obvious which are the optimal strategies for both players and a game-theoretic approach would be enlightening.

Now that the strategies have been described, although not explicitly defined yet, it is only the payoff function than remains to be presented. As expected, it is a function that is affected by the tolerance, the number of sensors that the defender decided to adopt and the number of attacks that the attacker decided to perform. This function denotes the payoff of the attacker and it is with the help of this function that a payoff matrix will be populated. The function for the attacker's payoff (AP) is:

$$AP = \left(\frac{is}{ts} \geq t\right) \cdot rcn + s \cdot cps - a \cdot cpa + t \cdot tc \qquad (7)$$

where, is = incorrect sum (i.e. the sum of significance coefficients of the actually compromised sensors), ts = total sum (i.e. the sum of significance coefficients of all sensors), t = tolerance, rcn = reward for compromising the network, s = number of sensors, cps = cost per sensor, a = attacks, cpa = cost per attack, tc = tolerance cost and:

$$\left(\frac{is}{ts} \geq t\right) = \begin{cases} 1 & if\ the\ inequality\ holds \\ 0 & if\ the\ inequality\ does\ not\ hold \end{cases} \quad (8)$$

As the formula denotes, the attacker will only be rewarded with rcn if she manages to compromise the network ($is/ts \geq t$) which is equivalent to [$(is/ts \geq t) = 1$], whereas she bears the cost of attacks, regardless their impact. Since the players are antagonistic, the attacker takes advantage of the defender's expenses. Thus, everything that has a cost for the defender, like the total cost of sensors ($s\times\ cps$) or the total tolerance cost ($t \times tc$) , is added to the attacker's reward in formula (7). The necessity of tolerance cost lies in the fact that the greater the tolerance is, the greater part of the whole information, should be faulty in order for it to be "believed". That motivates the attacker for a more comprehensive attack and therefore a less possible recovery by the operators of the network. Under this perspective, it could be preferable for the network to suffer a mild assault that will compromise the network temporarily, than risk suffering a massive one that will render it totally useless or unaffordable to be fixed. It should be noted that the payoff function has no units of measurement. It is just a necessary quantification of the advantage derived for each player due to the actions taken so that the problem can be solved and resembles the role of a utility function.

It is worth noting that although the defender is not aware of which piece of information is compromised, he is still able to use the outcome of formula (7). In other words, although the defender cannot distinguish between correct and faulty data, he is aware of the payoff that he receives when both players choose specific strategies. Furthermore, there is a chance that $(cs/ts) < (is/ts) < t$, where cs = correct sum. In this case, the compromised information will not be believed (although it is greater portion of the total information than the correct information is) and therefore no reward for compromised network is given to the attacker, which makes this situation relatively beneficial for the defender because although he will not be able to figure out which piece of information is correct and which not, he will be aware that he is under attack which gives him the option to not take any information from the sensors into account and therefore the attacker will not be awarded with rcn. Later on, this state will be called Middle State and obviously, it is only possible for $t > 0.5$ (50%).

Procedure Outline

In order for the game to be solved the optimal strategies have to be found. In practice, those strategies are represented by the strategies that constitute the Nash Equilibria (pure ones in our case). As explained in previous chapter, the existence of such pure Nash Equilibria will also mean that there are specific strategies, not necessarily one dimensional, that the players can follow and if they do so, none of them will be tempted to unilaterally change their strategy. That implies that the game has a "steady state" [37][38]. These Nash Equilibria will be found in this section with a rather complex way since the defender has two parameters that affect his strategy which makes the latter, a two dimensional one.

Since every strategy of the defender consists of a pair (m,n) where m is the number of sensors and n is the acceptable tolerance, it is not a typical case of game with two one-dimensional strategy sets and a two-dimensional payoff matrix. One way for this to be tackled and thus for the optimal strategies to be found, is the procedure that is adopted in this project and also in [37][38], although in our case it is more complex. The procedure is as follows. Firstly, the number of sensors is quantified and takes values in a predefined set. In this case, the number of sensors varies from 500 to 600 which is considered a realistic number for large areas. After the number of sensors is specified, a significance coefficient is generated for each sensor. Two cases have been considered about these coefficients. According to the first one, they are all equal to each other and according to the second one they are assigned values that follow a predefined distribution. Two distributions will be examined as part of this scenario. The Uniform(1,4) and the Normal(2.5, 0.25). Uniform distribution was chosen because it expresses a random assignment of significance coefficients and Normal due to its popularity based on the frequency that this distribution is met in various phenomena. Both are commonly used to describe various elements of network activity [118][119]. More about the employment of their parameters will be mentioned in the results analysis. The model can be easily modified so that those values follow any other distribution. After the number of sensors and the significance coefficients have been set, we will be left with many "standard form" games with two one-dimensional strategy sets remaining and a two-dimensional matrix. That can now be solved "traditionally" in order for the equilibria to be found. For this

project, the number of attacks lies in the interval from 400 to 600 while tolerance values vary from 0.55 to 0.9 or from 55% to 90%. The number of attacks takes values close to the ones of the number of sensors since it is realistic to assume that when an attacker wants to attack a network, she usually knows or can approximately estimate the number of sensors that comprise it and adapts the attacks accordingly. In the case where the number of attacks that the attacker decides to fire is greater than the sensors, it is assumed that all sensors are attacked. Of course, all of those attacks will bear the corresponding cost and not only the necessary ones. The following figure visualises the game for better observation of the reader.

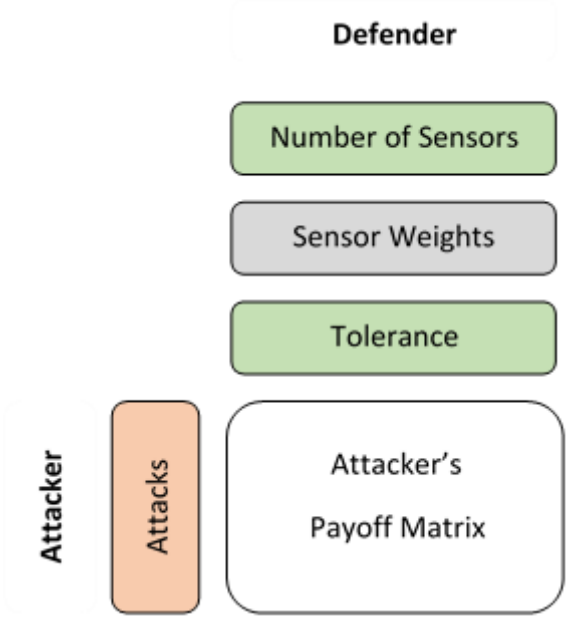


Figure 5: Visualized concept of the Intrusion Detection System, Sensor Weights not part of defender's strategy

In this figure, green colour denotes the parameters that are chosen by the defender and constitute his strategy ("Number of Sensors" and "Tolerance") while orange is used for the parameter that is chosen by the attacker and constitute her strategy ("Attacks" which is the number of attacks performed). Sensor weights are the aforementioned significance coefficients of the sensors which can shape defender's strategy, but their values are not chosen by the defender and therefore it is in grey colour. The aforementioned procedure will be followed for all the possible numbers of sensors and

all three scenarios for the values of significance coefficients (i.e. the significance coefficients being all equal to 1, following Uniform(1,4) and following Normal(2.5, 0.25)). Since the latter is not part of the defender's strategy, those three scenarios will be examined as individual cases.

These parameters shape the values of Attacker′s Payoff (formula (7)) which populate Attacker′s Payoff Matrix that is seen in Figure 5. This is the matrix of the game, based on which we will later look for Nash Equilibria.

The pseudocode of the approach that described above is the following:

$for\ s = S_{min}\ to\ S_{max}$

$SC(all\ sensors) = 1/follow\ Uniform(1,4)/follow\ Normal(2.5, 0.25)$

$Given\ the\ strategy\ sets\ for\ Number\ of\ Attacks\ and\ Tolerance\ level$

$-\ populate\ APM_s\ based\ on\ formula\ (7)$

$-\ calculate\ ne(APM_s)\ and\ AR\big(ne(APM_s)\big)$

$end\ for$

$NE = \{ne(APM_s), \forall s\}$

$AR(NE) = \{AR(ne()), \forall\ ne() \in NE\}$

$NEG = \big\{ne(APM_s) \in NE\ such\ that\ AR\big(ne(APM_s)\big) = min\{AR(NE)\}\big\}$

$Find\ which\ strategies\ lead\ to\ NEG$

where s is the number of sensors in the network, S_{min} and S_{max} are the minimum and maximum possible number of sensors, respectively, $SC()$ denotes the significant coefficient of deployed sensors, APM_s is the Attacker's Payoff Matrix (Figure 5) that occurred for $number\ of\ sensors = s$, $ne()$ is the Nash Equilibrium/a of a sub-game, $AR(ne())$ is the attacker's reward that corresponds to $ne()$ and NEG is the Nash Equilibrium/a of the whole game.

Results

Scenario 1: All significance coefficients are equal to 1 (all sensors equally trusted)

Assuming that the following parameters that affect the model are assigned the values: Sensors: [500, 600], Tolerance: [0.55, 0.9], Attacks: [400, 600], rcn = 10, cpa = 1.2, cps = 2.3, tc = 10 the plots below are derived. Those numbers can be considered realistic in a sense that the rcn and tc should be indeed considerably higher than cpa and cps respectively in order to motivate the attacker to perform massive attacks to compromise the network and discourage the defender from employing very high tolerance that could more easily lead to the Middle State mentioned earlier (which although is considered relatively beneficial for the defender, as already explained, it is still not as good as having a properly working "healthy" network).

In this section, we present our models' simulation results visualized as a triple graph.

As we know, for every possible number of sensors there is a different game that occurs. When this game has a pure Nash Equilibrium the attacker's and defender's strategy that constitute it can be found as well as the value of this particular game which is the payoff of the attacker when both players follow the aforementioned strategies. This is exactly what is depicted in the below triple graph.

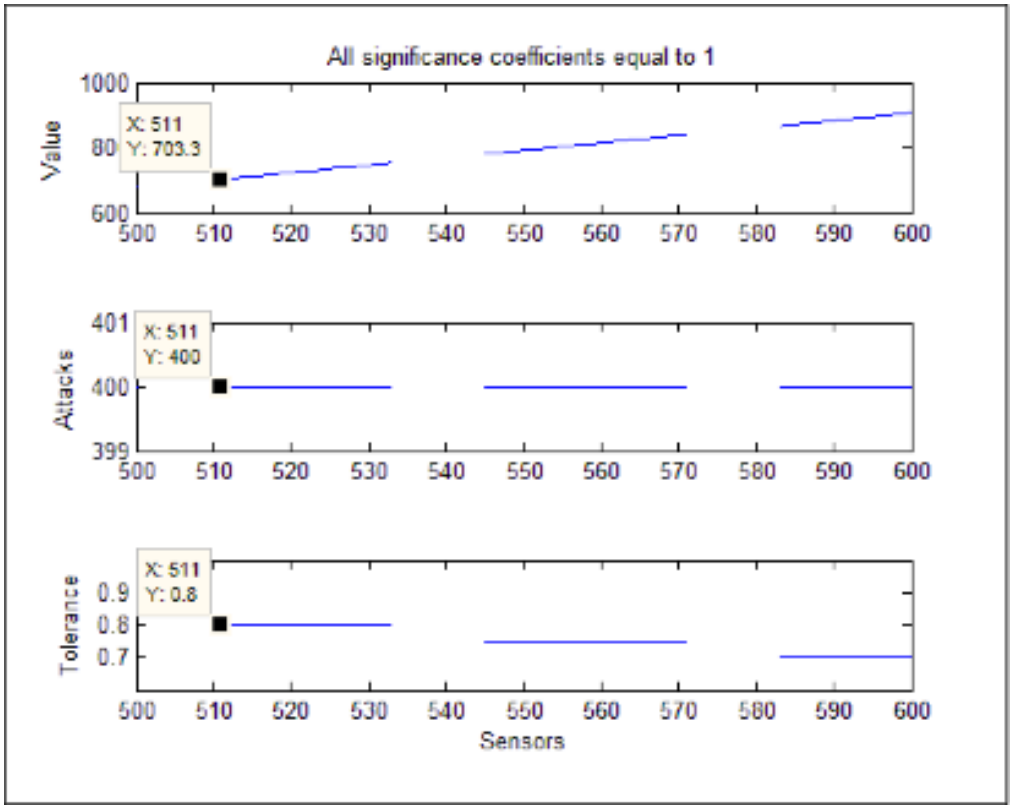


Figure 6: Game Value (Attacker's Payoff), Num. of Attacks and Tolerance for the NE that occurs for every

We interpret the figure, bearing in mind that we help defender to take the best possible decision regarding the maximisation of his payoff. In this figure, we can see the Nash Equilibria of all the sub-games that occurred. The horizontal axis in all sub-graphs of the figure is the number of Sensors. A Nash Equilibrium can be seen, as a vertical line that goes through all three sub-figures. If (x,y_1), (x,y_2) and (x,y_3) are the points that this line cuts the blue lines of sub-figures 1, 2 and 3 (starting from the upper one) respectively, that means that the best option for the defender would be to deploy x sensors and tolerance equal to y_3 for the WSN. The best response to that for the attacker is to perform y_2 attacks. That strategy would lead to a payoff for the attacker equal to y1. The pair (x,y_3) represents the best strategy that the defender can choose in order to respond to attacker's y_2 strategy and vice versa. Since every vertical line that goes through all sub-figures is a Nash Equilibrium (among the values of x that the graphs exist), we want the one that leads to

the least payoff for the attacker which is represented by y axis in the top sub-figure. Since the scope of the project is to help the defender make the optimal choices so the interpretation and exploitation will be made with respect to his interests. Therefore, given that the values of the first top sub-graph of the figure represent attacker's benefit, the best decision for the defender is to opt for the number of sensors that will *guarantee* the least of those values. The least possible attacker's payoff is 703.3 which is achieved when the defender deploys 511 sensors (x axis) in a WSN with tolerance equal to 0.8 (bottom sub-figure) and the attacker performs 400 attacks (middle sub-figure). Thus, the defender's optimal strategy is $(x, y_3) = (511, 0.8)$ and the optimal strategy for the attacker is $y_2 = 400$. This leads attacker's payoff equal to 703.3.

It should be noted that not all sub-games have a pure Nash Equilibrium and this is the reason behind the discontinuity of the graphs. Therefore, we conclude that when the number of sensors lies in the set $S = [500, 511) \cup (533, 545) \cup (571, 583)$ the corresponding games have no pure Nash Equilibria. Although there is no pure Nash Equilibrium for the games with number of sensors that belong in the set S, there is a chance that the defender will receive even greater payoff if he chooses for a number of sensors in this set. But this payoff would be by no means guaranteed and given that all players are considered rational and therefore risk-averse, they should seek the Nash Equilibrium strategies that lead to the best guaranteed payoff.

Based on the previous figure, one can see that no parameter of those three (i.e. Tolerance, Sensors and Attacks) can be changed unilaterally and lead to a better payoff. Indeed, if the optimal strategy set changes into another but the Number of Sensors remains unchanged, this will not lead into a better payoff because for this Number of Sensors the current Nash Equilibrium led to the optimal value of 703.3. If the Number of Sensors changes, then this will lead either to another Nash Equilibrium among the ones depicted and thus the Game Value will be reduced or to a game with no Nash Equilibrium that the defender should avoid because he is assumed risk averse due to his rationality. It is worth mentioning that this holds even if Number of Sensors and Tolerance change simultaneously which is possible since they co-create defender's strategy. As a result, the vector (511, 0.8, 400) represents the Nash Equilibrium of the whole game and the defender is advised to employ 511 sensors and a tolerance equal to 0.8.

This whole analysis will not be presented in all other examples for different distributions, but this logic is the same for all these cases.

Scenario 2: Significance coefficients follow a predefined distribution

In a similar way as in the previous scenario, similar figures with equivalent meaning will be created. Those are the following:

Distribution: Uniform (1,4)

For the following two cases, the values of the initial parameters (i.e. rcn, cpa, cps and tc) are the same as before.

The multiple graph for the case where significance coefficients follow Uniform(1,4) distribution is:

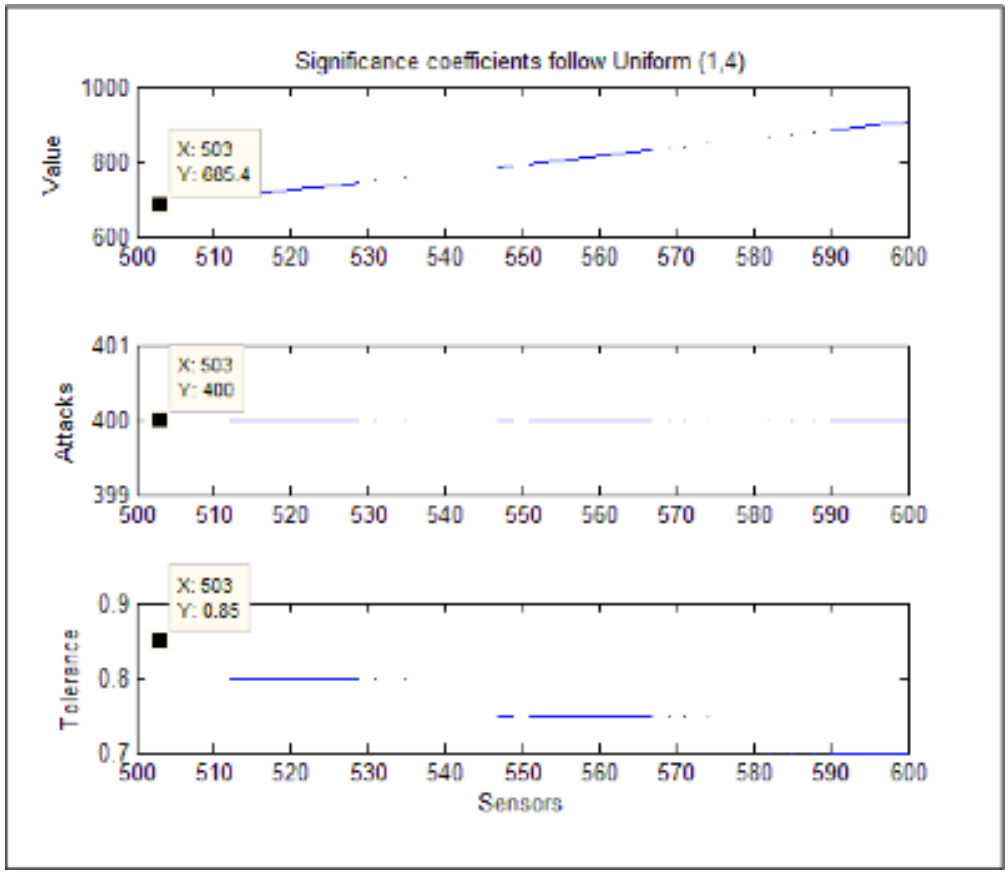


Figure 7: Game Value (Attacker's Payoff), Num. of Attacks and Tolerance for the NE that occurs for every

Sig nificance coefficients were chosen to vary from 1 to 4 because variance in not expected to be too high among them since all sensors are in the same field. Following the same logic as in the case with equal significance coefficients, the number of sensors that the defender should choose is 503. This will lead to the optimal strategies: 400 attacks for the attacker and 0.85 tolerance for the defender. When these strategies are chosen, the payoff of the attacker will be equal to 685.4.

Distribution: Normal (1,4)

The multiple graph for the case where significance coefficients follow Normal(2.5, 0.25) distribution is:

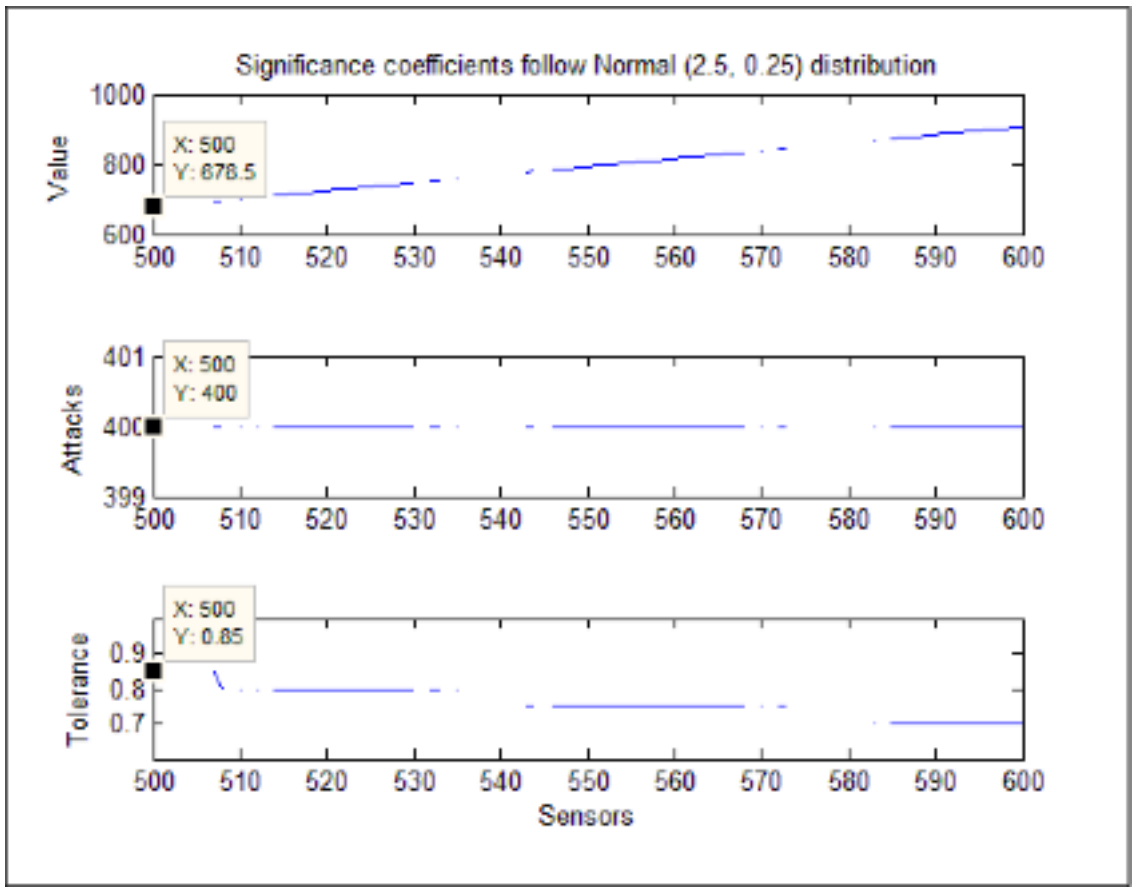


Figure 8: Game Value (Attacker's Payoff), Num. of Attacks and Tolerance for the NE that occurs for every

In a similar fashion to the previous cases, the number of sensors that the defender should choose is 500. This will lead to the optimal strategies: 400 attacks for the attacker and 0.85 tolerance for the defender. When these strategies are chosen, the payoff of the attacker will be equal to 678.5.

These numbers are very close to the case where the significance coefficients follow Uniform(1,4). That could partially be due to the fact that the Normal(2.5, 0.5) distribution takes values that belong to the interval $[\mu - 3\sigma, \mu + 3\sigma] = [1, 4]$ with probability 99.7% [120] The mean and variance of Normal distribution were chosen that way so that a direct comparison with the case of Uniform distribution is possible. However, the change of those values usually changes the results only a little and especially the number of sensors.

It should be taken into account that all the figures presented for all cases result from numerous iterations and that the last two models require the generation of random numbers which could lead to slightly different results every time those models are tested. It is worth noting that the points that constitute the optimal strategies in the final two figures are not easily observable because they are individual points. Below there is an aggregated table with all the results of this section.

Table 3: Cumulative results for the Intrusion Detection System

Intrusion Detection Model			
Significance Coefficients	Optimal # of Sensors	Optimal Tolerance	Optimal # of Attacks
All equal to 1	511	0.8	400
Uniform(1,4)	503	0.85	400
Normal(2.5, 0.25)	500	0.85	400

3.2.2.2 Intrusion Prevention System

With so many possible kinds of data for collection by the sensors and assumptions regarding the attacks, the detection and/or defense mechanisms and even the operation of the WSN, it is obvious that the possible use cases are practically endless. For simplicity, it is assumed that the use case under investigation is similar to the previous one (i.e. wireless sensors that measure temperature and an attacker that tries to inject faulty data to them under the aforementioned assumptions). Regarding the model itself, although this

one, compared to the previous one, has some major differences that are demonstrated below, some elements are still the same. There are still a defender and an attacker where the first one owns or operates a WSN and the second one tries to undermine it. Since this is an IPS and not an IDS, it is assumed that detection of attacks is not an issue any more and all of them are known to the defender. As before, both the attacker and the defender have strategy sets that depend on some parameters. However, now both players have two parameters that define their strategies, unlike the previous case where the defender had two (number of sensors and tolerance) but the attacker had only one (number of attacks). The attacker can now choose the distribution (and its mean value) that the number of attacks will follow while the defender can choose the number of sensors that the network will consist of as well as the number of recoveries that will be made. It is important that the attacker does not choose the exact number of attacks but only the distribution and mean value that the amount of attacks will follow. The ability of the defender to recover compromised sensors is a critical change that causes severe differences to the way the model progresses and essentially demands a whole new approach do be designed and implemented. Finally, the acquisition and/or installation of the sensors, the recoveries and the attacks come with a cost and since there are adversarial interests involved, Game Theory is again an appropriate tool to be used.

The games and sub-games presented in this section will be once more two-player, zero-sum, non-cooperative games but there will be two different versions. One of them will be the static (or one-shot) game version where, the game only consists of one round and the other one will be the iterated version where the game consists of a predefined number of rounds and every round starts from the state that the previous round was finished. Essentially, the first version is an instance of the second for one iteration.

Non – iterated game

As mentioned, this is a game comprised from a single round where the attacker has to choose the distribution (and its mean) that the number of attacks will follow while the defender has to choose the number of sensors that constitute the network and the number of recoveries that will be made.

The formula adopted for the attacker's payoff is the following:

$$AP = a \cdot (rcs - ac) + r \cdot (rcps - rcs) + s \cdot sc + \left(\frac{a-r}{s} \geq t\right) \cdot rcn \qquad (9)$$

where,

$$\frac{a-r}{s} \geq t = \begin{cases} 1, & if\ inequality\ holds \\ 0, & if\ inequality\ does\ not\ hold \end{cases} \qquad (10)$$

and AP = Attacker's Payoff, a = number of attacks, rcs = reward for compromising a sensor, ac = attack cost, r = number of recoveries, $rcps$= recovery cost per sensor, rcs = reward for compromised sensor, s = number of sensors, sc = sensor cost and rcn = reward for compromising the network.

Both the number of attacks and number of recoveries are restricted within an interval of possible values. The term rcs appears twice because every time a recovery takes place, the attacker's reward per compromised sensor is essentially canceled.

In this payoff formula, it is crucial that some prerequisites are met in order for the model's solution not to be obvious. Firstly, if the term $(rcs - ac)$ is a positive one, then the more attacks the attacker would decide to do, the more her payoff would increase. Therefore, there would be no reason for her not to attack as many sensors as possible. Similarly, if the term $(rcps - rcs)$ is negative then the more recoveries the defender would choose to do, the less payoff the attacker would receive and that would always lead to a solution which would impose that the defender should always perform as many recoveries as possible. Thus, the inequalities: $rcs < ac$ and $rcps > rcs$ should hold in order for the optimal strategies to not be obvious. Although those ensure that the number of attacks and the number of recoveries will not always take their highest possible values, there should also be a reason that those parameters will not always receive their lowest possible values as well, otherwise the solution of the problem (i.e. its Nash Equilibrium) would be obvious. This is ensured by the term:

$$\left(\frac{a-r}{s} \geq t\right) \cdot rcn \qquad (11)$$

where the reward for compromised network will, obviously, be a positive number. This product, as part of the payoff function, motivates the attacker to opt for more and more attacks and the defender to opt for more and more recoveries while the previous properties push for the opposite. This does not mean that it is impossible for the solution of the problem to be found to force one or both of those variables to take their highest or lowest possible values. It is just not obvious, from a mathematical perspective, that something like this would always happen when the aforementioned requirements are met. From now on, this set of requirements will be referred to as Requirements for Non-Obvious Solution (RNOS).

Procedure Outline of the Non-Iterated Game

In this section, the whole procedure of finding the optimal strategies for the game described above is outlined and the pseudocode is presented. It is not possible for the method that was followed in the intrusion detection system to be adopted in this case also, before some necessary changes that address the specificities of the problem take place.

Initially, the intervals that the involved parameters lie in should be defined. In the version that the results demonstrated later are based on, the number of sensors can take values between 200 and 400, the number of attacks takes values between 10 and 120 and the number of recoveries is valued between 1 and 70. The range of the number of attacks matters, although not part of the strategy, because this range denotes the capabilities of the attacker. Due to that, the mean values of all the distributions will fall in the same range as the number of attacks. The distributions of the number of attacks are Normal, Exponential and Poisson.

The method behind finding the Nash Equilibrium in this game is the same as in the IDS section although now there is one more dimension in the strategies, because the attacker has two parameters that affect her strategies instead of one, and it is probably less obvious than before that the solution found in this way is indeed a Nash Equilibrium. However, when the suitable plots are demonstrated, the whole logic becomes clearer.

The desirable outcome will be a result of the following algorithm:

- Initially, the variable that denotes the number of sensors iterates through the whole interval of possible values (from the minimum to the maximum).
- For every possible number of sensors, the (nominal) variable that denotes the followed strategy iterates through the set of possible strategies (i.e. Normal, Exponential, Poisson).
- For all the above parameters fixed, it is only the parameter of mean values and the one that represents the recoveries that are still unspecified. With only those two parameters still free to take their permitted values, the game will be solved and any possible Nash Equilibria will be found. The payoff that corresponds to the combination of specific values for recoveries and distribution/mean, occurs as follows. For every possible distribution, a variable that denotes the mean of the already chosen distribution iterates through the possible values and for every possible mean number, there are 5 random generated numbers that are generated in a way that they follow the already fixed distribution with the fixed mean.
- The Nash Equilibria that were found by the said algorithm are then plotted in order for final outcomes to be derived.

The figure below is demonstrated in order to clarify things more for the reader.

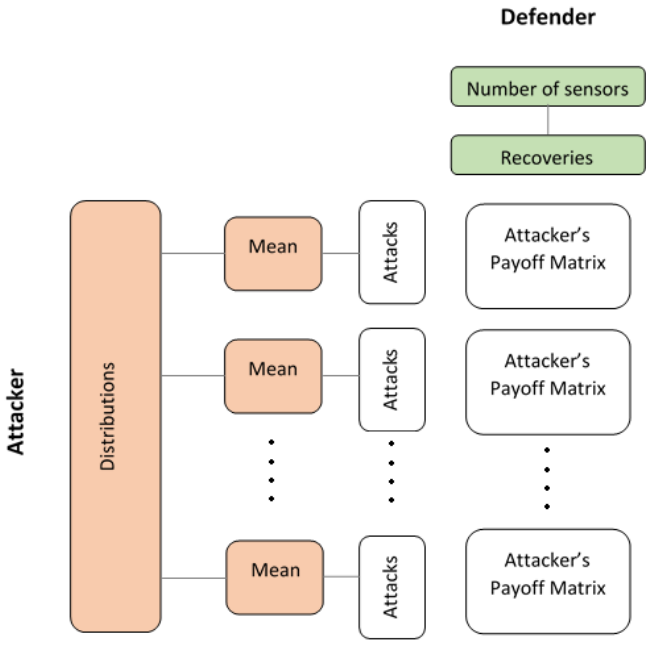


Figure 9: Visualized concept of the Non-Iterated Intrusion Protection System, Number of attacks not part of attacker's strategy

Before the aforementioned plots are demonstrated, the pseudocode of the algorithm previously described is given.

$for\ s = S_{min}\ to\ S_{max}$

$for\ every\ D \in Distributions = \{Normal, Poisson, Exponential\}$

$for\ every\ m \in MeanValues$

$-\ Generate\ Attacks(i),\ i = 1, \dots, 5\ that\ follow\ D(m)$

$-\ Let\ Attacks(i),\ i = 1, \dots, 5\ be\ possible\ values\ of\ "Number\ of\ Attacks"$

$Given\ the\ strategy\ sets\ of\ attacks\ and\ recoveries$

$-\ Populate\ APM_s\ based\ on\ formula\ (9)$

$-\ Calculate\ ne(APM_s) and\ AR\big(ne(APM_s)\big)$

$end\ for$

$end\ for$

$end\ for$

$$NE = \{ne(APM_s), \forall s\}$$
$$NEG = \left\{ne(APM_s) \in NE: AR\left(ne(APM_s)\right) = min\{AR(NE)\}\right\}$$
$$Find\ which\ strategies\ lead\ to\ NEG$$

where, MeanValues is the set of all possible mean values and is described later on. By D(m) we mean that the variable follows distribution D with mean m. In the case of Normal distribution, there is also variance (σ^2) needed but is omitted from the pseudocode for simplicity. However, it is taken into account in the execution of the real code. That variance remains unchanged through the model and has been chosen in a way such that all the values that are generated and follow N(m,σ^2) lie within the defined range. In addition, the procedure of generating attacks has been designed in a way such that $\{attacks\ that\ follow\ D(m_i)\} \cap \left\{attacks\ that\ follow\ D\left(m_j\right)\right\} = \emptyset, for\ i \neq j, \forall\ D\ \in Distributions$.

Results of the Non-iterated Game

The plots depicted below were derived when the model run for the following prices: Sensors: [200, 400], Recoveries: [1, 70], Distribution of number of attacks: Normal, Poisson, Exponential, rcs = 1.5, ac = 3, Mean values created per distribution = 5, rcps = 5, sc = 4, rcn = 2000, t = 0.5, Attacks: [10, 120]. Apart from being proportionally realistic to each other, those numbers also meet all the Requirements for Non-Obvious Solutions (RNOS) that apply on them. Interpretation of Figure 10 is almost identical to the one of

Figure 6, Figure 7 and Figure 8. The only difference is that there are now all three distributions in the same figure. Therefore, the Nash Equilibrium of this game will be the one that leads to the minimax price (i.e. the minimum price out of the highest possible ones) of "Value". Given that every vertical line that goes through all sub-figures is a Nash Equilibrium of the game and (x,y_1^i), (x,y_2^i), (x,y_3^i), i ∈ {Normal, Poisson, Exponential} are the 9 points that this line cuts sub-graphs 1, 2 and 3 then if the defender chooses a specific number of sensors x, the attacker will choose as a response, out of points $\{(x,y_1^i)$, i ∈ {Normal, Poisson, Exponential}$\}$ the distribution i for which max$\{y_1^i$, i ∈ {Normal,

Poisson, Exponential}} is achieved. Thus, assuming that (x, y_1^i) are the points that the vertical line that goes through x cuts all graphs of the first sub-figure, the defender should choose x for which $\min_x\{\max_{y1}\{\text{ordinate}(x, y_1^i)\}\}$ is achieved. The strategies that correspond to the points found that way, form the Nash Equilibrium of the whole game since they follow the definition of Nash Equilibrium mentioned earlier.

By choosing the strategies in that way the resulting strategies form the set (Number of Sensors, Number of Recoveries, Distribution, Mean) = (200, 1, Exponential, 92.5) with a attacker's payoff equal to 780.1. For the same reasons as in the previous model, the whole game cannot have a Nash Equilibrium with Different number of Sensors. Considering that variable fixed, a unilateral change of strategies would mean one of the following:

Case 1

A change in the Number of Recoveries that will lead to non - Nash Equilibrium which is to be avoided by rational players;

Case 2

A change in the Distribution that will lead to an already plotted Nash Equilibrium which, given that the number of sensors is still 200, will not lead to an attacker's payoff greater than 780.1;

Case 3

A change in the mean value which will not lead to Nash Equilibrium; or finally

Case 4

A simultaneous change of the Distribution and the mean value (that is possible because those two together constitute attacker's strategy) which will lead either to a plotted Nash Equilibrium with attacker's payoff less than 780.1 or to no Equilibrium at all. The reasoning behind all those was explained in the IDS section.

To sum up, the vector of strategies (Number of Sensors, Number of Recoveries, Distribution, Mean) = (200, 1, Exponential, 92.5) is a Nash Equilibrium because no unilateral strategy change is beneficial for the player who will opt for it. Hence, the

advised strategy to the defender is to employ 200 sensors and almost no recoveries (only one). Obviously, these results would be different if the parameters were given different values, as well.

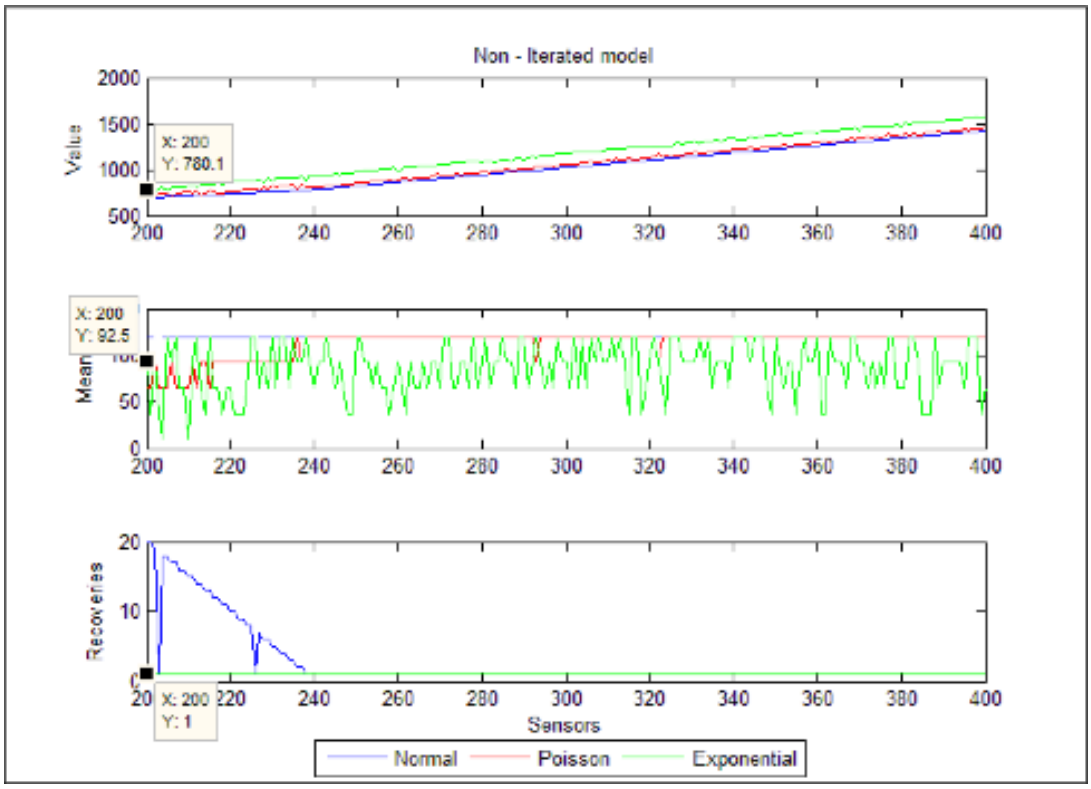


Figure 10: Game Value (Attacker's Payoff), Mean values and Number of Recoveries of the Nash Equilibria

Iterated Game

The iterated version of the game is practically the same as the previous one, with only some small differences due to the fact that it is repeated for many rounds. The payoff function for the attacker is now:

$$AP = ta \cdot (rcs - ac) + tr \cdot (rcps - rcs) + s \cdot sc + \left(\frac{cse}{s} \geq t\right) \cdot rcn \qquad (12)$$

where ta = total attacks, tr = total recoveries, cse = compromised sensors, after final round (for all three of them) and all the other variables are the same as in the non-iterated model. As usual:

$$\frac{cse}{s} \geq t = \begin{cases} 1, & if\ inequality\ holds \\ 0, & if\ inequality\ does\ not\ hold \end{cases} \quad (13)$$

Total attacks and total recoveries are defined as follows:

$$total\ attacks = \sum_{i=1}^{n} attacks\ at\ round\ i \quad (14)$$

And

$$total\ recoveries = \sum_{i=1}^{n} recoveries\ at\ round\ i \quad (15)$$

where n is the predefined number of rounds. The procedure outline and therefore its pseudocode, is the same as in the non-iterated model with the difference that now the beginning state of every round (i.e. the number of compromised and uncompromised sensors) is the ending state of the previous one. The optimal strategies will be of the same form as in the non-iterated game (i.e. a single value for optimal number of attacks and a single value for optimal number of recoveries), because both of strategies are decided in the beginning of the game and remain the same for all rounds. What this game-theoretic approach helps us find is the optimal strategy for the players to follow in order to have the best possible outcome at the end of the game. We can therefore say that even the iterated game is a static one although in a repeated form.

Results of the Iterated Game

For all the same parameter values as in the non-iterated scenario and for 20 iterations, the following figure depicts the results. Even rcn remained the same although it is now more difficult for an intruder to compromise a network, but this happened so that comparison can be made.

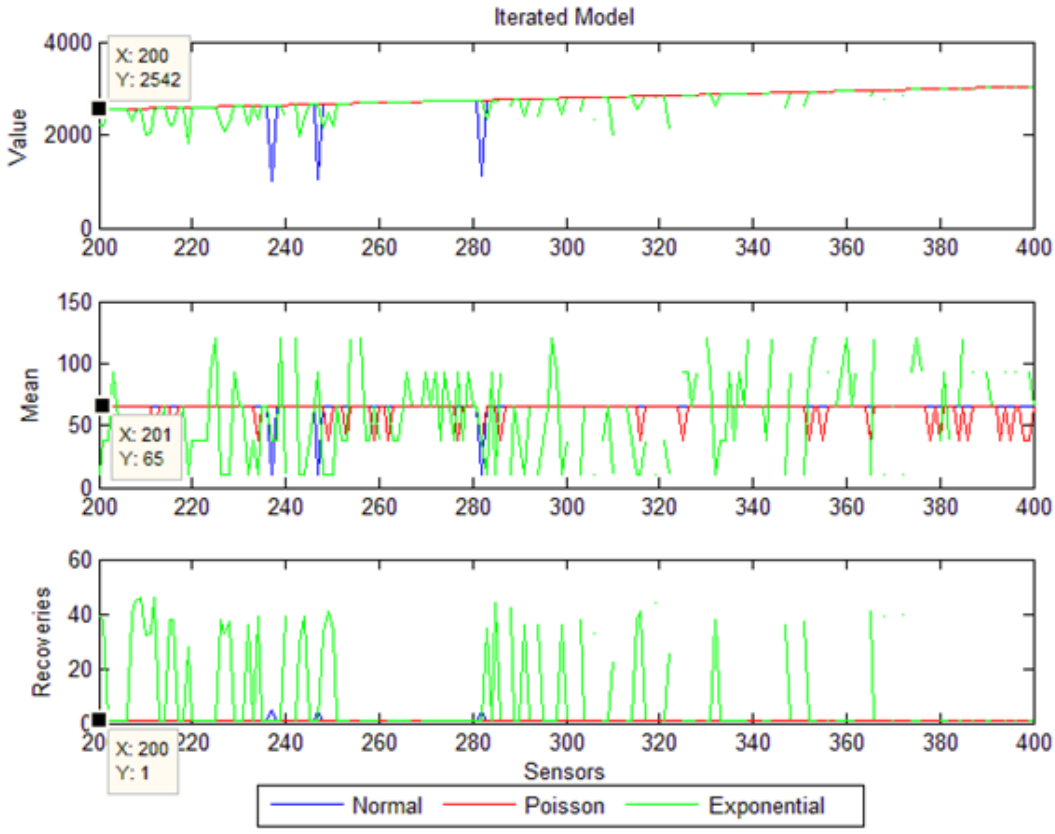


Figure 11: Game Value (Attacker's Payoff), Mean values and Number of Recoveries of the Nash Equilibria

Following the same way of interpreting this figure, the defender would be advised to employ 200 sensors and make just one recovery per round (the least possible amount). That would lead to a payoff for him equal to -2542 (attacker's payoff is depicted and it is a zero-sum game).

Below there is, again, an aggregated table with all the results of this section.

Table 4: Cumulative results for the Intrusion Prevention System

Intrusion Prevention Model			
Type	Optimal # of Sensors	Optimal # of Recoveries	Optimal Distr. of Attacks
Non-Iterated	200	1	Expon.(mean: 92.5)
Iterated	200	1	Poisson (mean: 65)

Comments on the results

Judging from the top sub-graph of Figure 10, it can be concluded that all distributions appear to have almost the same behaviour. The way that the parameters were set, seems to have great impact on the behaviour of both players. In particular, the attacker does not seem motivated enough to try to compromise the network since this target is not plausible enough. Additionally, it is also the fact that the whole game lasts for just one round that renders the attacker's target of compromising the network rather improbable. Even if Normal Distribution (that seems to have the greatest mean of attacks) is adopted, the result is disappointing due to the high number of recoveries. Exponential and Poisson distributions, despite their relatively high mean of attacks, do not manage to compromise the network and their payoff value remains a lot lower than 2000 which would be the reward for this achievement.

A one round game may seem doomed, but one would expect that this would not be the case for the 20-round game. And things do change for all distributions since they all end up with payoffs for the attacker above 2000, which is an indication of a compromised network because this payoff would be difficult to be raised otherwise. The relatively high number of mean values for all distributions and low value of recoveries (with the exception of Exponential which scores a little less in the end) in conjunction with the duration of 20 rounds make attackers motivated enough. However, it should not be forgotten again that mean values are not necessarily equal to the actual number of attacks.

The reason that both models are included in the project is that comparison can be made and conclusions can be drawn about the way the players react based on the number of the rounds they are allowed to have. In this case, this parameter had a major role in the outcome although rcn remained the same in both cases

3.2.3 Validation in a Cluster-Based Deployment

In this section, we conduct a number of experiments to validate both the IPS and the IDS utilising the clustering facilities offered by SensomaX which allows us to validate our simulation with a hardware-in-the-loop approach.

SensomaX [121][122] is an agent-based WSN middleware, which supports concurrent execution of multiple applications, integrates different mechanisms for different operational paradigms, and facilitates application developers with a component-based architecture for seamless development process. SensomaX is written in Java and was modified to be used on various java-enabled hardware devices such as the Raspberry Pi. One its features is a hierarchical communication mechanism, which abstracts the network into logical regions with exclusive functionalities. In SensomaX, each application is allocated a region according to its needs, whilst resources in the same region can be utilised by other applications simultaneously. However, each application's concurrent utilisation of the network resources is completely invisible to other applications. Such capability could also create a multi-tier and collaborative execution environment where multiple applications' interaction using the same set of hardware resources is necessary.

Using SensomaX, end-user applications physically interact with the network through a gateway. In the gateway, there exists a layer known as the Assessment Layer with a principle component called the Agent Examiner (AE). This layer provides a simple XML parsing tool in order to split the application requirements and label them with their relevant application sources. In the next step, those requirements submitted by different applications are processed and broken down into a single or multiple agents, based on their demands and complexity. This sort of top-layer processing is the result of two components' coordination: Task Engine and System configuration.

In all our experiments, both models (IDS and IPS) were programmed as two separate applications in every sensor node. Those two applications can be executed concurrently in order to detect and prevent attacks, whilst sensor nodes are carrying out their normal operation and meeting the requirements of their given task. The application itself resides in a single node, known as the Cluster-Head, where all the top-level executions happen. The IDS and IPS applications (i.e. model logic) are present in every sensor node, whilst being executed only in the Cluster-Heads.

For the first phase of our experiment a network of 600 virtual nodes was created in SensomaX Companion Simulator (SXCS) [123], incorporating 30 clusters, each containing 20 nodes. As a way of a sensing application, all nodes were programmed to constantly report Temperature readings at 1-second intervals. A second network

containing 600 nodes without any clustering mechanism was also created to report false temperature readings. Each experiment reported in this section was repeated 100 times to gain the average values. Figure 12(a) demonstrates the average number of attacks required before detection. For a 510-node network, the average number of attacks is 398. This result is on par with the results reported in

Figure 6, given the standard deviation, which covers the 400 attacks reported earlier. Figure 12(b) depicts the number of nodes required for the IPS model to operate successfully based on a variable number of attacks. The results reported in this figure are also relatively on par with the results reported in Figure 11 given the standard deviation around the mean values. The impact on the energy consumption of the network is depicted at Figure 12(c).

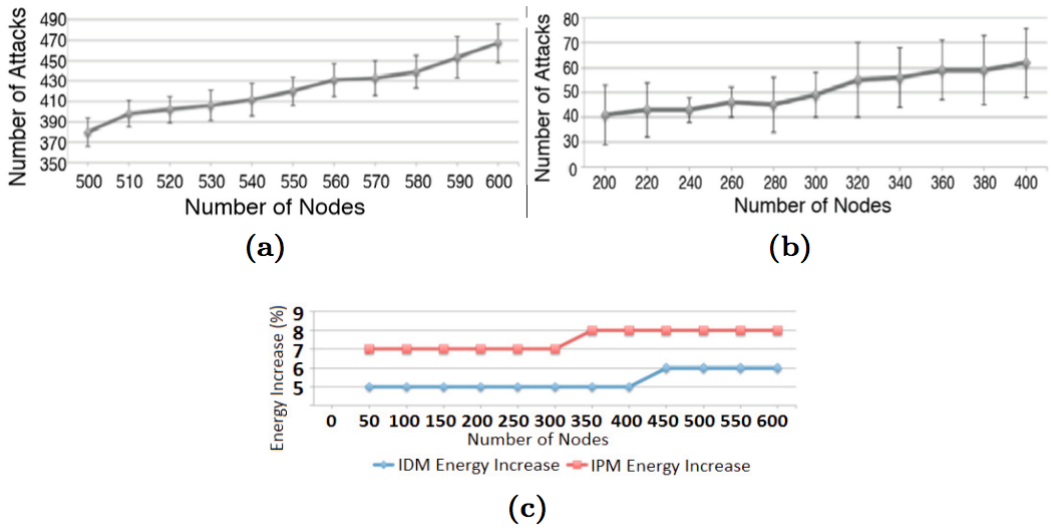


Figure 12: (a), (b) IDS's & IPS's required number of nodes vs. number of attacks, respectively, (c) Impact of IDS & IPM on energy consumption

3.2.4 Validation in an IPv6-Based Deployment

In this section we make use of Cooja [124], the network simulator distributed with the Contiki Operating System for the Internet of Things. Within Cooja, we simulate an IPv6-based wireless sensor network. Network nodes use IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [125] and the Routing Protocol for Low Power and Lossy Networks (RPL) [126]. We simulate a network with 1 traffic sink and 40 traffic

sources, distributed in a 200x200 grid. Node distribution is entirely random, with the only limitation being that all sources must have a network path to the sink. We choose to simulate a network of 40 nodes in order to achieve full area coverage, as is the assumption in the model. We use 10 different random topologies and for each topology we repeat the experiment 10 times using a new random seed for each iteration.

In the remainder of the section, we use the following notation: n is the index of a node, $N = \{n: n \in Z + \wedge\, n \leq 40\}, C = \{n: n \in N \wedge node\ n\ is\ compromized\}$, t is the defender's chosen tolerance, $D_n: n \in N$ is the degree of node n discussed below, $S_n: n \in N$, is the significance of node n, also discussed below. In the model, the choice of node significance is based on a random distribution. In our simulations, we model node significance as a function of network density. We first calculate the node degree D_n for each network device, which is calculated as the number of other network nodes within communication range. The significance S_n for node n is subsequently calculated as $S_n = \max(\{D_i: i \in N\})/D_n$.

Thus, S_n corresponds to the maximum node degree observed in the network, divided by the node's own degree. Since, all nodes in the network have a path to the sink, they have at least one other node within communication range. Hence, $D_n > 0$ and the significance calculation's denominator is always non-zero. This way, nodes in dense areas will have lower significance, while nodes in sparse areas will have a high one. That is because the network is used to gather sensory information about an environmental parameter in a geographical region. Even between two identical devices, measurements are likely to be slightly different due to manufacturing inaccuracies and slight fluctuations of environmental parameters even within the same area. Thus, in an area where multiple nodes are reporting, each node's measurement will be of lower significance, whereas in a sparse area where only a few nodes are reporting, it will bear more weight.

According to the model, the optimal attacker strategy is to compromise 78.27% of the total number of nodes in the network (400 out of 511). With this in mind, in each experiment the attacker compromises a random set of 31 nodes ($|C| = 31$). Furthermore, defender's optimal strategy is to select tolerance level T = 0.85. An attack is successful if the defender believes the erroneous value to be accurate and this is only true if $Attack's\ coefficient\ (AC) = \sum_{j \in C} S_j / \sum_{i \in N} S_i > T$.

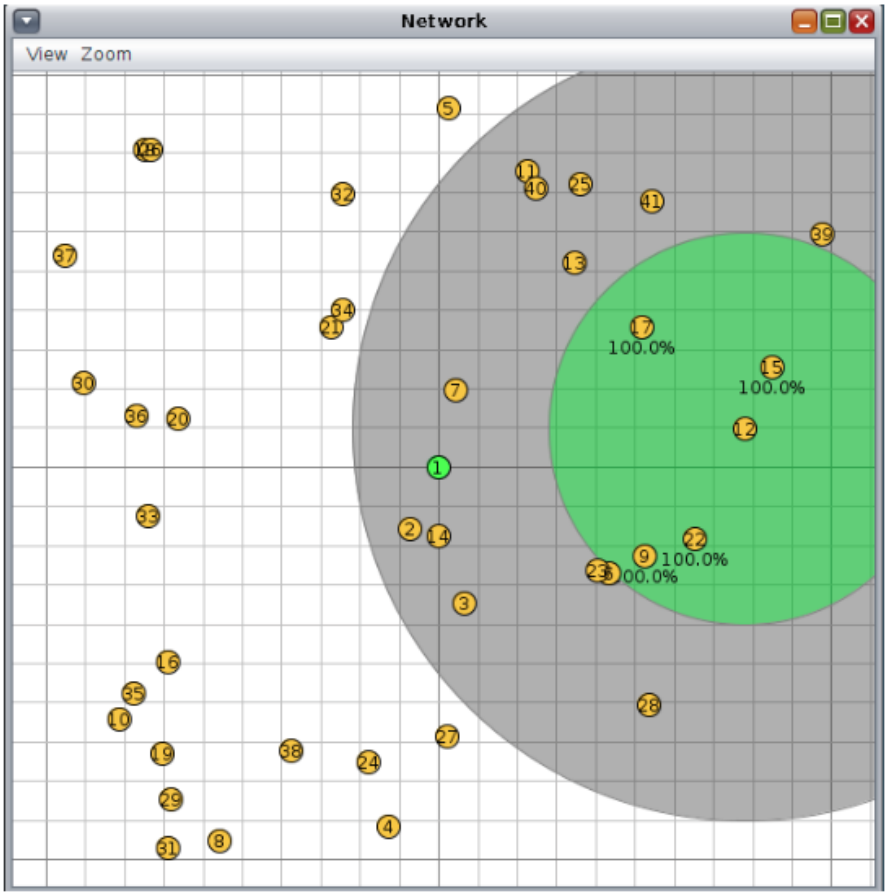


Figure 13: Network set-up in Cooja

Figure 13 illustrates an instance of the network set-up in Cooja. Figure 14 illustrates the densities of the ten network deployments under investigation. For all deployments, the minimum node degree Dn was between 1 and 3, whereas maximum node degree was between 7 (topology 1) and 13 (topologies 3 and 5).

Figure 15 illustrates attack coefficients for each iteration. Across the entire experiment set the attacker was successful only three times. For all other iterations' detection was possible. The three successful attacks were observed in topologies 3 and 5, i.e. the ones with the highest network density. This suggests there may be a relation between the model's accuracy and the network density. This can be further investigated in future.

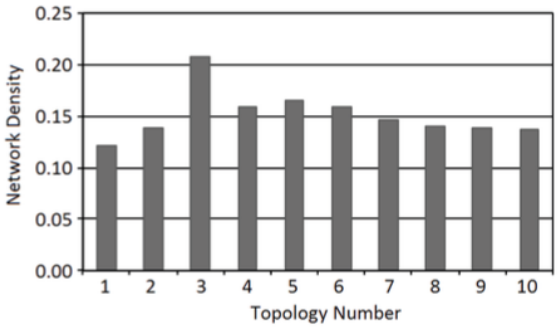


Figure 14: Topology densities

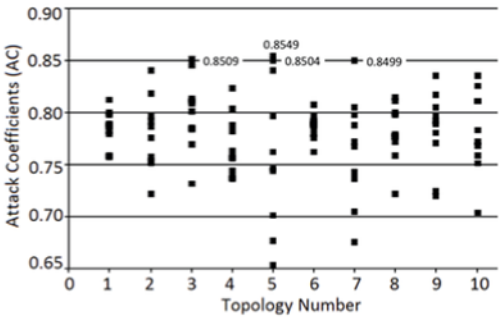


Figure 15: Attack Coefficients per experiment

3.2.5 Findings and Conclusions

In this work, we demonstrated how Game Theory can be used to detect and prevent intrusions in WSNs. The proposed models, which are applicable on a wide range of use cases, including IoT applications, smart metering and others, were also validated using two methods of validation. The first validation method used SensomaX while the second one used Cooja with which the effectiveness of the IDS in an IPv6-connected network of smart objects was investigated. In both validation cases, the results confirmed the ones of the analytical models.

Another idea for future improvement is to extend the model in order to include forecasting, applied on the iterated game with multiple rounds. By fixating the parameters and running the aforementioned iterated game for many different numbers of rounds, we could apply forecasting methods in order to make an approximation of a player's payoff, given the number of iterations. Furthermore, we aim to investigate its applicability on networks of varying densities as well as its scalability with increasing network size.

3.3 Critical Infrastructure – Industrial Control Systems (CI-ICSs)

In this section there are some novel approaches about systems' security and risk management applied on CI-ICSs. The presented use cases are categorised, according to the tools they use, to those that i) combine VSM and Game Theory, ii) use Monte Carlo predictive modelling or iii) combine Game Theory and Epidemiology. Details of these models are presented below.

3.3.1 CI-ICSs Security using VSM and Game Theory

Traditional cyber-security risk management methods are based on the evaluation of risk which is affected by the likelihood of cyber-security incidents occurring [127], [128]. However, these probabilities are usually estimations or guesses based on past experience or incomplete sets of data [129]. Incorrect estimations can lead to errors in the evaluation of risks that can ultimately affect the protection of the system. This is inherited to risk management methods used in ICSs, as they are mainly adaptations of such traditional approaches. Additionally, conventional methods fail to adequately address the increasing threat environment and the highly interdependent critical nature of ICSs, while proposed methods by the research community are yet far from providing a solution [19], [130]–[132]. The importance of managing securely ICS infrastructures is growing, as they are systems embedded in critical national infrastructure (e.g. city traffic lights controls) and thus an emerging attractive target for organized cyber criminals and terrorists. In this section, we present two novel approaches that combine Stafford Beer's VSM [133] with Game Theory in order to develop a risk management process that addresses the above issues. The model we develop provides a holistic, cost-efficient cyber-security solution that takes into account interdependencies of critical components as well as the potential impact of different attack strategies.

3.3.1.1 VSM on CI-ICSs - Case study 1

The content of this section addresses part of RQ2 by expanding on our approach that combines VSM and Game Theory in order to provide cost-efficient defence solutions for CI-ICSs, that take into account their complex interdependencies.

For the purposes of our research we utilised the VSM to capture the relationships between the cyber components of an ICS and also those between the components of different ICSs. In that way, after the identification of the cyber components within the ICS, we assess the value of each component, taking into account the cascading effect of its failure to the rest of the components, within both the same and different ICSs. Assessing the value of each component through its interconnections helps us identify the impact of having it disrupted or destroyed.

In order to model the interconnections, we adopt an agent-based approach. Each cyber component is modelled as an agent characterised by its market price, its input and output connections with other cyber component agents and with the environment, the type of its function in correspondence with the VSM structure (System 1, System 2 etc.) and the VSM level that it belongs according to its recursive feature. Figure 16 depicts how a cyber component within an ICS is modelled.

In order to compute each component's value, we have to answer the following questions:

- What is the initial market price of the component?
- Which VSM Level does it belong to?
- Which other ICSs is it indirectly connected to?
- What is its role (System x) within the VSM (operational unit, coordination unit, auditing unit etc.)?
- How many environmental entities does it take input from?
- How many entities in its environment does it provide output to?
- How many other cyber components does it take input from?
- How many other cyber components does it provide output to?

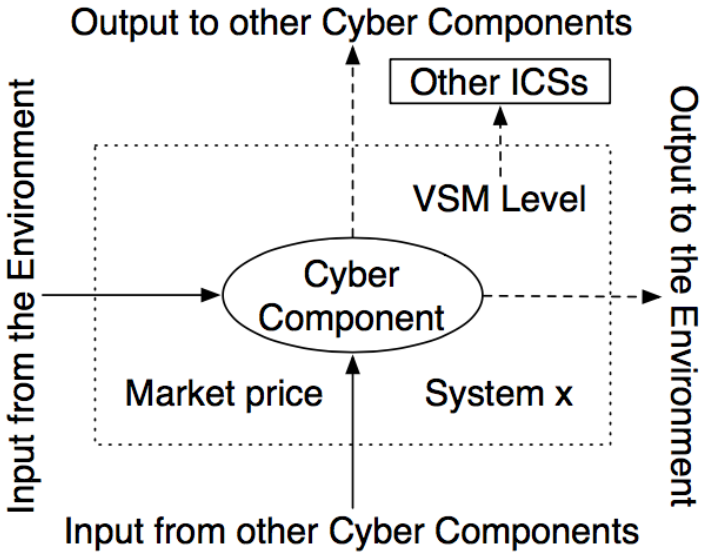


Figure 16: An ICS Cyber Component

Answering those questions for every cyber component, provides us with a way to determine their importance to the whole system. The number of total connections and the importance of the component's role form a factor, which multiplied by the initial market price of the component returns the ultimate value of the component. The VSM level refers to the recursion level that the cyber component belongs to and provides information on its purpose within the ICS and the way it affects other ICSs. For example, a Programmable Logic Controller (PLC), which is a control device used in many ICSs, is an operational unit (System 1) within a VSM of level *n*. Along with other field devices it may compose the production department of a power production station. The production department itself is the operational unit within a VSM of level *n*-1. Along with the other departments it may construct the organisational structure of the power production company. Considering this structure as a VSM of level 1, we now have *n*-1=1. Therefore, the PLC belongs to a VSM of level *n*=2. A power plant in its turn affects other ICSs since it provides the electricity they need to function. Therefore, the PLC has a level 2 effect on other ICSs. The magnitude of this effect is proportional to the role of the PLC (System 1) and the number of other devices with the same role in the same VSM level. The quantification of the role of each cyber component depends on the enterprise's perception of each role's importance. A quite simplistic yet acceptable, at this point of our work, way to compute the real value of a cyber component is by multiplying its various

characteristics: ***Value*** *= (Market price) x (Number of connections) x (Effect on other ICSs) x (Role of the cyber component),* where, ***Effect on other ICSs*** *= (Role of the cyber component) / (Number of devices with the same role and VSM level)*

To demonstrate how we embed GT in our model, we present a game scenario where an attacker (e.g. a hacker) plans an attack against a critical infrastructure (e.g. a power supply plant) while a defender (e.g. plant's operators) is responsible for the best possible protection under limited resources (e.g. funds). The possible scenarios are practically endless. Below, we will examine a use case where a PLC device is under attack. The attacker and the defender can be considered as players, the whole scenario as a game and all their possible actions as strategies.

Due to the structure of the model, in order for a game-theoretical tool to be used, those strategies have to be identified, their impact has to be assessed and finally their probabilistic interdependencies to be evaluated. These steps are no other than Threat/Vulnerability Identification, Threat/Vulnerability Assessment and Risk Evaluation, respectively; steps that constitute the Risk Assessment of our scenario. As the outcome will be the proposal of specific strategies for the players, it is an integrated Risk Management use case.

The parameters that define attacker's strategies are the adoption or not of espionage, the core security attribute that the attack aims at (Confidentiality, Integrity or Availability), the inveteracy of the vulnerability that the attack targets at (less than one year which describes a zero-day threat or more than one year), the level of difficulty of the attack's detection (very difficult in case of multiple zero-day threats, difficult in case of a single zero-day threat or easy in case of attacks with older than one year threats) and the level of difficulty of the attack's recovery (very difficult if it requires a hardware replacement, difficult if it requires a system patch or easy otherwise). Similarly, the parameters that define defender's strategies are the employment or not of a Research and Development (R&D) department for security problems, the frequency that the patches are applied with (yearly, more than a year or never) and the existence or not of an IDS.

Let's assume a scenario where the cyber asset under attack is a PLC device. We assume that the market price of the PLC along with its installation is 15000, the number of connections within the ICS is three, a sensor that feeds it with data, a mechanical device, such as a valve, that is controlled by the PLC and the Supervisory Control And

Data Acquisition (SCADA) server that connects the PLC with the Control Centre. Its role is to control (System 3) the valve in the VSM level 3 and operate as a unit (System 1) in VSM level 2. Due to its dual purpose the value of the asset is increased by two. In this work we will exclude the effect of interdependencies with other ICSs but this is something that can be added in future. Thus, the ultimate value of the PLC is: *Value* = 15000 ×3×2 = 90000. The rest values attached to the parameters, presented in Table 5, represent our perception of the specific problem and can be easily adapted to the needs of any ICS.

Apart from the strategies, there are also the rewards of each player that need to be defined for any possible combination of strategies. Below are the formulas employed for attacker's rewards. We assume that the reward of a player is the loss of the other (zero-sum game), therefore the identification of one player's rewards is sufficient.

Table 5: Attack Coefficients per experiment

Attacker's Strategies		
Espionage		30,000
Security Attribute	Confidentiality	0.33
	Integrity	1
	Availability	1
Inveteracy of Vulnerability	<1Year	1,000
	>1Year	10
Difficulty of Detection	Very difficult	4
	Difficult	1
	Easy	0.5
Difficulty of Recovery (Cost of Healing)	Very Difficult	101,000
	Difficult	1,000
	Easy	10
Defender's Strategies		
R&D		10,000
Patch Frequency	Never	0
	1 Year	1,000
	>1 Year	100
IDS		10
Value of Asset Under Attack		90,000

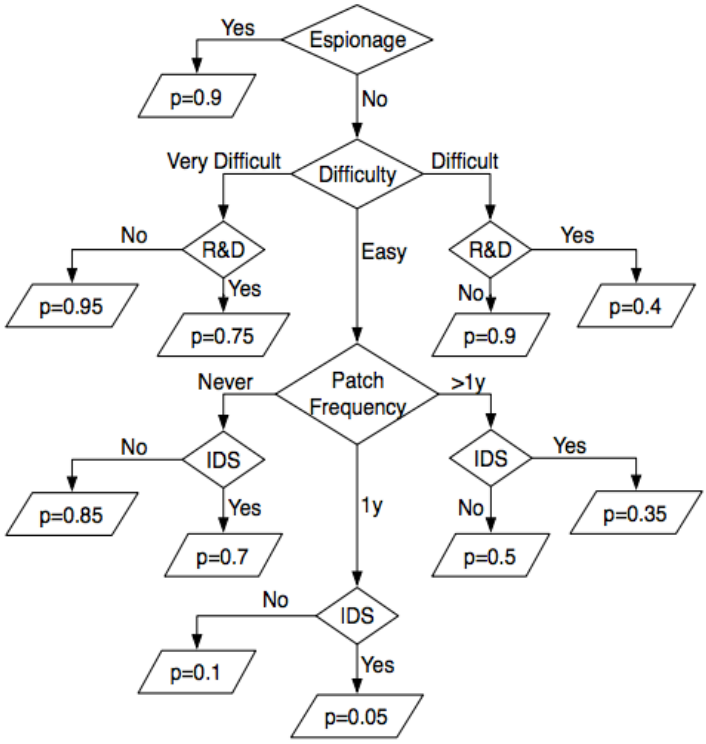


Figure 17: Flowchart of probabilities of successful attack

Attacker's Reward = *Gain + Cost of Defence + Cost of Healing – Cost of Attack*

Where,

Gain = *Value of Asset × Security Attribute × Probability of Successful Attack*
(for Probability of Successful Attack given by Figure 17.)

Cost of Defence = *R&D + Patch Frequency + IDS*
Cost of Healing = *Difficulty of Recovery*
Cost of Attack = *Espionage + Inveteracy of Vulnerability × Difficulty of Detection*

Taking also into consideration the following assumptions:

- Attack against C cannot be very difficult to recover
- Zero-day attack cannot be easy to detect
- >1Years attacks can only be easy to detect

and adding also the case of not attacking within the strategies of the attacker's strategies (the case of not defending is already included in the defender's strategies and it is equivalent to adopting no defence mechanisms out of the proposed ones), we end up with a 43×12 table of rewards. The game is solved by identifying its Nash Equilibria, which is a commonly adopted concept of a game's solution.

Results

This game was found to have two Nash Equilibria that are presented in the format:

A: (Attack, Espionage, Core Attribute, Inveteracy of Vulnerability, Difficulty of Detection, Difficulty of Recovery)

D: (R&D, Patch Frequency, IDS)

The Nash Equilibria are:

A: (Yes, No, Integrity, 1 Year, Very Difficult, Very Difficult)

D: (Yes, > 1 Year, No) and

A: (Yes, No, Availability, 1 Year, Very Difficult, Very Difficult),

D: (Yes, > 1 Year, No)

Both lead to a payoff of 174,600 for the attacker, which is equivalent to 174,600 loss for the defender under our assumptions.

It is worth mentioning that if the three aforementioned assumptions had not been implemented, then we would have ended up with a larger table of rewards and thus, maybe with even more Nash Equilibria. However, these Nash Equilibria would be based on unrealistic requirements and we would therefore exclude them anyway.

Findings and Conclusions

This work presents a novel approach towards cyber security risk management in ICSs. Combining the VSM with GT we created a method that provides cost-efficient defence strategies that take into account the proprietary and interconnected nature of an

ICS. The proposed method requires the modelling of the ICS's cyber components as agents that represent systems in the VSM structure. In this way we quantify the criticality of an asset through its interconnections to other components. Then we construct a game between the attacker and the defender in order to compute the most cost-efficient strategies of both, when they compete upon each cyber component. Our model is generic and can be applied on many ICSs, regardless of its nature and function. Nevertheless, it can be further enhanced covering a wider range of defence and attack strategies, while validation against real data is also required.

3.3.1.2 VSM on CI-ICSs - Case Study 2

The content of this section addresses part of RQ2 by thoroughly presenting a novel approach that combines VSM with Game Theory in order to develop a risk management process which provides a holistic, cost-efficient cyber-security solution that takes into account interdependencies of critical components as well as the potential impact of different attack strategies.

Similar to the previous one, this model approaches an ICS as a VSM, as well. Each component within the system is represented as part of a VSM and carries the characteristics and connections that correspond to its particular purpose within the system. Thereby, the system can be modelled as an aggregation of interdependent VSM components with specific characteristics that contribute to the system's viability. The viability of the ICS is defined through a system of weighted components connected through weighted links. The weights in both cases reflect the purpose of the element in the VSM or in other words its importance to the system. Subsequently, we define the strategies of the two adversaries, extending the work of Levitin and Hausken [134], maintaining their systemic nature so that we can provide defence strategies against unknown threats. Eventually, we develop a two-player, zero-sum game with pure strategies. The defender's objective is to minimise the impact of a cyber-attack while minimising the security costs regardless of the attacker's move. This is achieved by following a strategic plan that represents the Nash Equilibrium of the game.

The VSM of ICS

Figure 18 presents an architectural block diagram of a typical ICS. The system is divided into three sections. The first part consists of the field devices, including devices used to control mechanical processes or transfer data from and to other devices (e.g. PLCs - that control the speed of a motor, Remote Terminal Units (RTUs) that exert wireless control on operations etc.). The second part forms the control centre, which exerts control on the field devices. It communicates with the field devices and includes operator workstations also known as Human Machine Interfaces (HMIs), data historians, databases etc. Finally, the third part of an ICS represents the outer world with which the system communicates.

In order to show how the various parts of an ICS can collectively form a VSM, we examine a simplified ICS version which includes three operations: 1) the control and monitoring of the speed of a motor, 2) the remote control and monitoring of a waste disposal unit and 3) the voltage control on a specific instrument used within the ICS. Figure 19 shows how this example can be presented as a VSM. As we see, the three operations are managed by a PLC, an RTU, an Intelligent Electronic Device (IED) and their corresponding sensors. Those elements form the components/operational units of System 1. Those components are controlled by the Control Centre which is an aggregation of machines (data historians, shared resources, HMIs etc.) that help controlling the various field devices. Therefore, the Control Centre forms System 3. The communication between the Control Centre and the field devices is managed through the control network and the use of a SCADA server. Therefore, the SCADA server forms System 2. The HMIs within the Control Centre are responsible for auditing the system. Thus, they play the role of System 3^{*}. Lastly, System 4 and 5 are realised through the Forward Planning Direction of the organisation and the Management Board respectively.

Measuring Viability

According to the VSM the viability of the system depends on its subsystems; the performance of each subsystem affects the whole system's viability. Therefore, to measure the viability of the system we need to calculate the performance of each element

(S2, S3, S3*, S4, S5 and operational units within S1 are considered as elements) within the system identifying (based on the VSM representation in Figure 19) the way interdependencies affect it.

We consider the performance of each element as gradual taking values from 0 (the element has stopped functioning) to *x* (the higher is *x* the better is the performance of the element). Its value depends on the element's functional capability, which refers to its performance before we take into account interconnections (normally this is equal to 1, "optimal performance"; values less than 1 would indicate some malfunction), and its connection to other elements (each connection is weighed from 0 to 1 according to its significance to the element's performance).

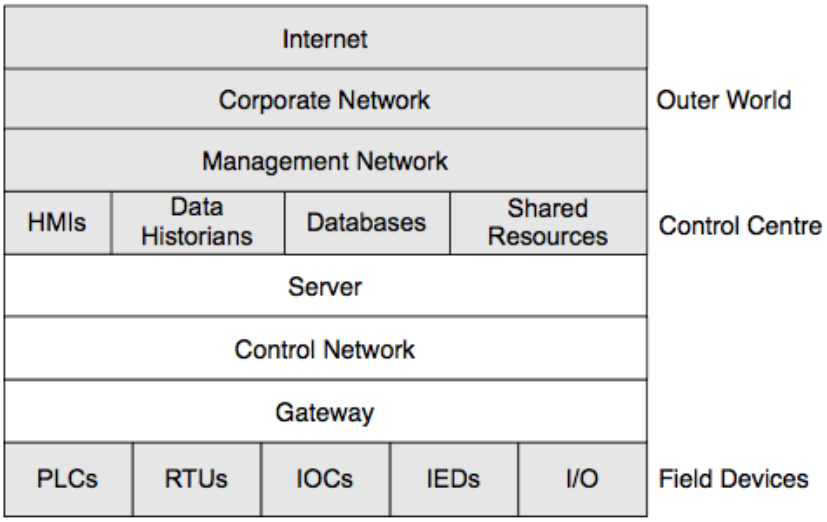


Figure 18: Simplified ICS architecture [135]

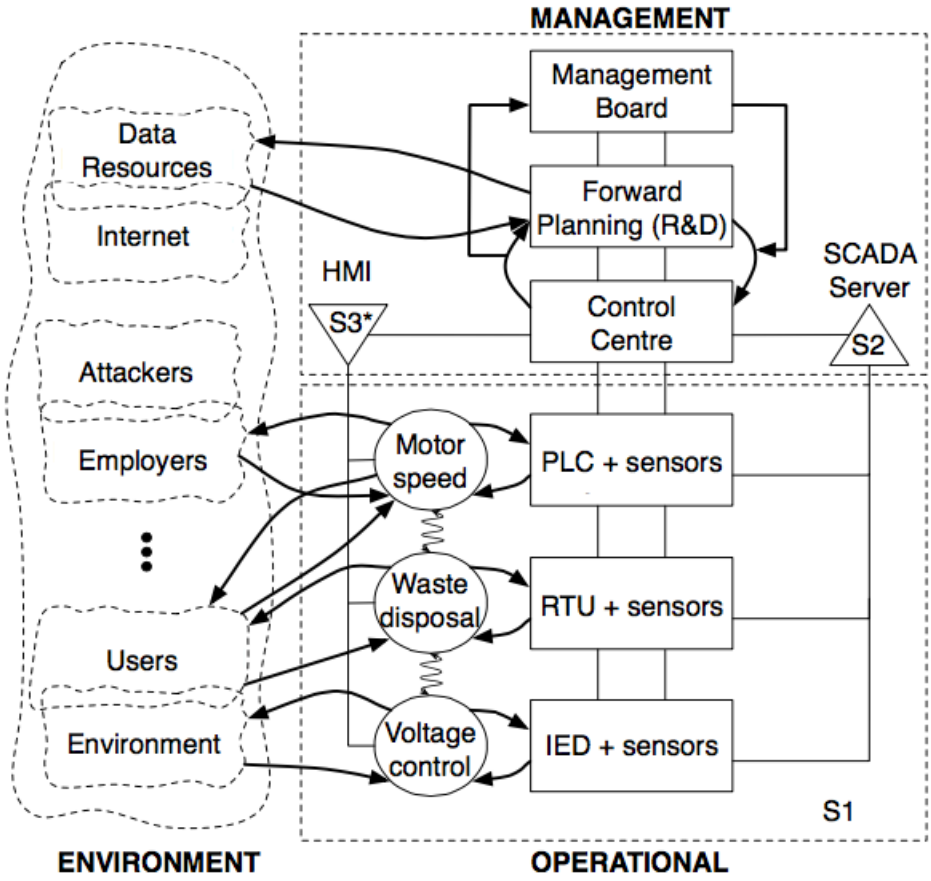


Figure 19: The VSM of an example ICS

Performance of Operational Units within System S1

Figure 20 emphasises on the interdependencies between an operational unit and the other systems within the VSM (it has to be noted that there is no communication between operational units in this level). A weight is assigned to each connection according to its significance to the unit's performance. Additionally, a performance value is assigned to each connected system. Based on that, Equation (16) calculates the performance of the unit taking into account its functional capability, its dependencies on other systems (S_2, S_3, $S_3{}^*$ and the environment) within the VSM and the performance of each connected system.

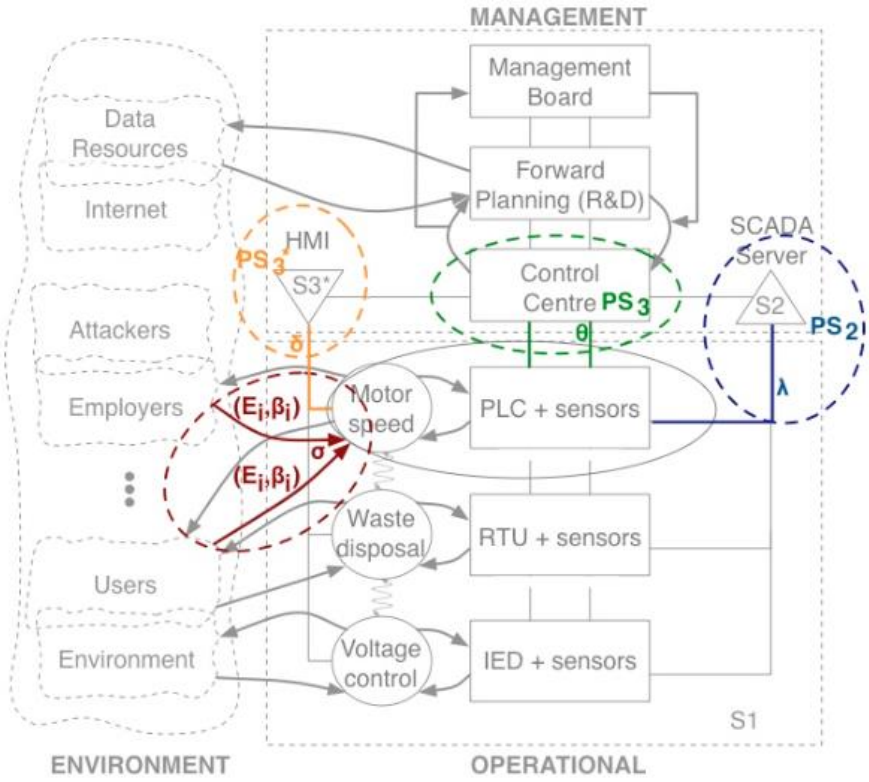


Figure 20: Dependencies of an operational unit

$$PU = FCU \cdot f(\sum_{i=0}^{n}(\beta_i \cdot E_i) \cdot \sigma, \lambda \cdot PS_2, \theta \cdot PS_3, \delta \cdot PS_3^*) \quad (16)$$

PU stands for the unit's performance and FCU represents its functional capability. E_i represents the input from environmental groups (under normal conditions this is considered equal to 1; values less than 1 would indicate issues in the connection with the environment), β_i is the weight assigned to the specific environmental input, σ is the significance of the total environment to the unit and n is the total number of environmental groups that communicate with the unit. PS_2 represents the performance of System 2 that coordinates the unit's communication within the VSM with weight λ, PS_3 stands for the performance of System 3 that controls the unit with weight θ and PS_3^* is the performance of the System 3* that audits the unit with weight δ. The coordination, control, and audit weights denote the significance of those functions to the performance of the unit. All weights take values from 0 to 1.

Taking into account that S_3 and $S_3{}^*$ cannot communicate with S_1 without the S_2, and also that S_3 (for control) and $S_3{}^*$ (for monitoring) are essential for S_1's operation, Equation (16) can be simplified in:

$$PU = FCU \cdot \left(\sigma \sum_{i=0}^{n} (\beta_i E_i) + \lambda PS_2 \cdot \theta PS_3 \cdot \delta PS_3^* \right) \quad (17)$$

Performance of System 2

Since System 2 is responsible for the connection of operational units in S_1 to the rest of the VSM. Its performance does not depend on other systems; it relies solely on the element's functional capability and is described by Equation (18)

$$PS_2 = FCS_2 \quad (18)$$

where $0 \leq FCS_2 \leq 1$ represents the functional capability of System 2.

Performance of System 3

The ability of System 3 to monitor and control the operations within System 1 depends on its connection to S_1 that is coordinated by S_2 and audited by $S_3{}^*$, and its communication with S_4. Thus, the performance of System 3 can be described by Equation (19)

$$PS_3 = FCS_3 \cdot f(\upsilon \cdot PS_2, \omega \cdot PS_3^*, \chi \cdot PS_4) \quad (19)$$

where FCS_3 is the functional capability of System 3, PS_2 corresponds to the performance of System 2, PS_3^*, corresponds to the performance of the System 3^*, PS_4 is the performance of System 4 and υ, ω and χ the respective weights that indicate the systems' significance to S_3's performance. All weights take values from 0 to 1.

Taking into account that S_2 and S_3^* are essential for S_3's operation (monitoring and control of S_1's operations), and that although S_4 adds to S_3's performance, it cannot be considered as vital, we simplify Equation (19) as:

$$PS_3 = FCS_3 \cdot \upsilon PS_2 \cdot \omega PS_3^* \cdot (1 + \chi PS_4) \quad (20)$$

*Performance of System 3**

System 3* is responsible for auditing the operations withinS_1. Its performance is therefore based on its connection to the S_1 which is realised through S_2. Thus, the performance of System 3* is:

$$PS_3^* = FCS_3^* \cdot f(\kappa \cdot PS_2) \quad (21)$$

where FCS_3^* is the functional capability of System 3*, PS_2 the performance of S_2 and $0 \leq \kappa \leq 1$ its weight depending on its significance to S_3^*.
Given the fact that without S_2 there is no communication between S_3^* and S_1 Equation (21) can be simplified in:

$$PS_3^* = FCS_3^* \cdot kPS_2 \quad (22)$$

Performance of System 4

The performance of System 4 depends on its connection to S_5 and although it does not depend on S_3, it takes data from the environment and after S_5 has processed them, they are sent back to S_3. Thus, it can be calculated as:

$$PS_4 = FCS_4 \cdot f(\alpha \cdot EI, \varepsilon \cdot PS_5) \quad (23)$$

where FCS_4 is the functional capability of System 4, EI represents the interaction with the environment (if such an interaction exists then EI = 1, otherwise EI = 0), PS_5 stands

for the performance of System 5 and α and ε are the corresponding weights. All weights take values from 0 to 1.

Given the fact that both S_5 and EI are essential for the operation of S4, the Equation (23) can be simplified in:

$$PS_4 = FCS_4 \cdot \alpha EI \cdot \varepsilon PS_5 \tag{24}$$

Performance of System 5

System 5's functionality is based on the knowledge it receives from System 4, and therefore its performance that represents its speed of decision is based on S_4's functionality as shown in Equation (25),

$$PS_5 = FCS_5 \cdot f(\mu \cdot PS_4) \tag{25}$$

where FCS_5 is the functional capability of System 5 (we consider this equal to 1 since we do not take into account ill management practices), PS_4 is the performance of System 4 and $0 \leq \mu \leq 1$ the corresponding weights.

Since in case S_4 is missing S_5's decisions cannot be applied in the lower levels of the system the Equation (25) can be simplified as:

$$PS_5 = FCS_5 \cdot \mu PS_4 \tag{26}$$

Total Performance

Modelling each element's performance according to their contribution to the VSM gives us an insight on how interconnections affect the performance of the system. From the equations provided above, we can observe that operations within System 1 depend on the performance of each element of the system. To ensure viability we have to ensure that elements (operational units) within S1 operate in their maximum possible performance.

Since the investigation of the effect of ill management and poor planning practices on the system performance are not in the scope of this work, we can consider PS_4 and

PS_5 to be constant; for simplicity we assume PS_4=PS_5=1. Thus, combining Equations (17), (18), (20), (22), (24) and (26) we have:

$$PU = FCU \cdot \left(\sigma \sum_{\iota=0}^{n} (\beta_i E_i) + \lambda FCS_2 \cdot \theta FCS_3 \cdot \upsilon FCS_2 \cdot \omega FCS_3^* \cdot \kappa FCS_2 (1+\chi) \cdot \delta FCS_3^* \cdot \kappa FCS_2 \right) \quad (27)$$

Since PU refers to the performance of one operational unit within S_1, and due to the fact that operational units are independent of one another, the total performance can be calculated as:

$$P_{total} = \Phi_1 PU_1 + \Phi_2 PU_2 + \cdots + \Phi_k PU_k \quad (28)$$

where k is the total number of operational units and Φ_i is the importance of each unit to the functionality of the whole system.

Defining Strategies

In order to overcome likelihood estimations of conventional risk management approaches we use game theory. By deploying a game between the attacker (cyberthreat actor) and the defender (ICS operator), both of which are considered as rational players (i.e. they both want to maximise their payoff taking into account the incurred cost), we can identify strategies for the defender that will return the optimal outcome (here defined as maximum system performance under the minimum cost) regardless the attacker's strategy.

We consider two types of defence methods for the defender. The first defence method we use is redundancy. In particular, the ICS operator needs to find the elements within the system to which redundancy should be applied in order to maximise the total performance while minimising costs. The cost of redundancy depends on the element (e.g. in an example where legacy systems are used within S_1while $S_3{}^*$ has been upgraded with modern systems, the application of redundancy is much easier in $S_3{}^*$ than S_1). The second type of defence is patching. In the same way with redundancy, the ICS operator needs to identify the elements within the system which should be patched in order to

maximise performance while minimising costs. The cost of patching depends again on the element (e.g. remote, inaccessible operational units and legacy systems are more difficult to patch). Via 'patching' we mean an essential software update that mitigates known vulnerabilities.

From the attacker's point of view, the strategies involved depend on the selection of the element that should be compromised (e.g. compromising the SCADA server - S_2 - may return a larger payoff compared to compromising a single operational unit within S_1) and the complexity of the attack that should be used (e.g. complex Advanced Persistent Threats (APTs) that include previously unseen 'zero-day' attacks, or exploit common vulnerabilities).

Deploying the Game

Our game is based on Equations (27) and (28). For the players' strategies we make the following assumptions:

- Attacks on elements are binary: successful (decrease the element's functional capability to 10%) or unsuccessful (the element's capability is not affected).
- Attacks can be deployed against multiple elements.
- Available attacks per element: common or zero day (one attack per element; no mixed attacks)
- Available defences per element: redundancy or patching (one defence per element; no mixed defences)
- Patching renders a common attack unsuccessful.
- A zero-day attack is successful against patching.
- Redundancy renders both zero-day attack and common attack unsuccessful.
- The cost of an attack-strategy depends on the number of elements to attack and the type of attack ($\text{Cost}_{\text{zero-day}} > \text{Cost}_{\text{common}}$).
- The cost of a defence strategy depends on the element type (e.g. applying redundancy or patching to S3 may be more expensive than applying them to S2) and the type of defence which in turn depends on the ICS Implementation

(e.g. redundancy may seem more costly but patching may require system reboot that - especially in the case of legacy systems - can also be costly).

- There could be a probability of patching failure but in this case it has not been taken into account. It only requires a very small change to the model though.

Figure 21, Figure 22, Figure 23 and Figure 24 provide the attack/defence trees for all elements on which the game is played. At this point we have to note that Figure 21 represents one element within the S_1; since we have k elements within S_1 (κ operational units in S_1) we also have k trees similar to Figure 21, one for each element/operational unit.

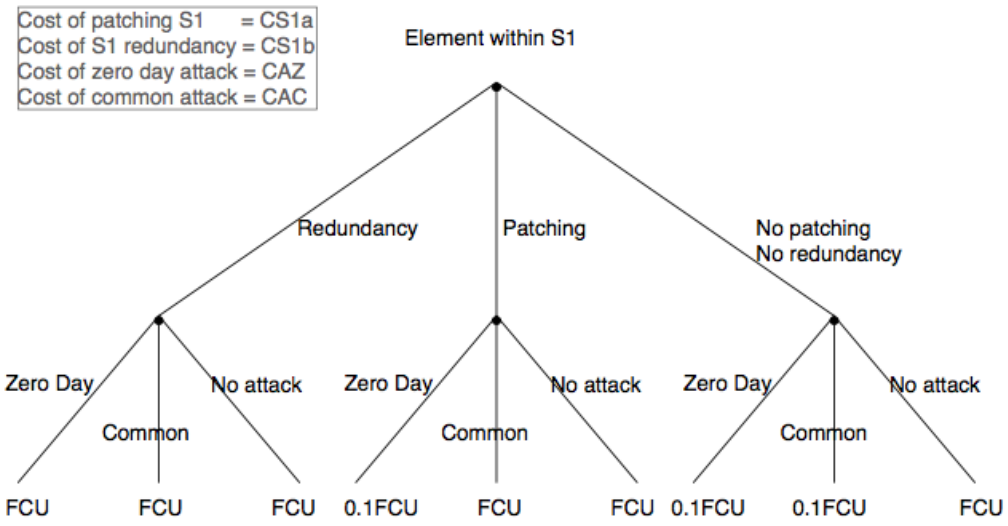


Figure 21: "Attack/Defence on element within S1" tree (one tree for each element within S1)

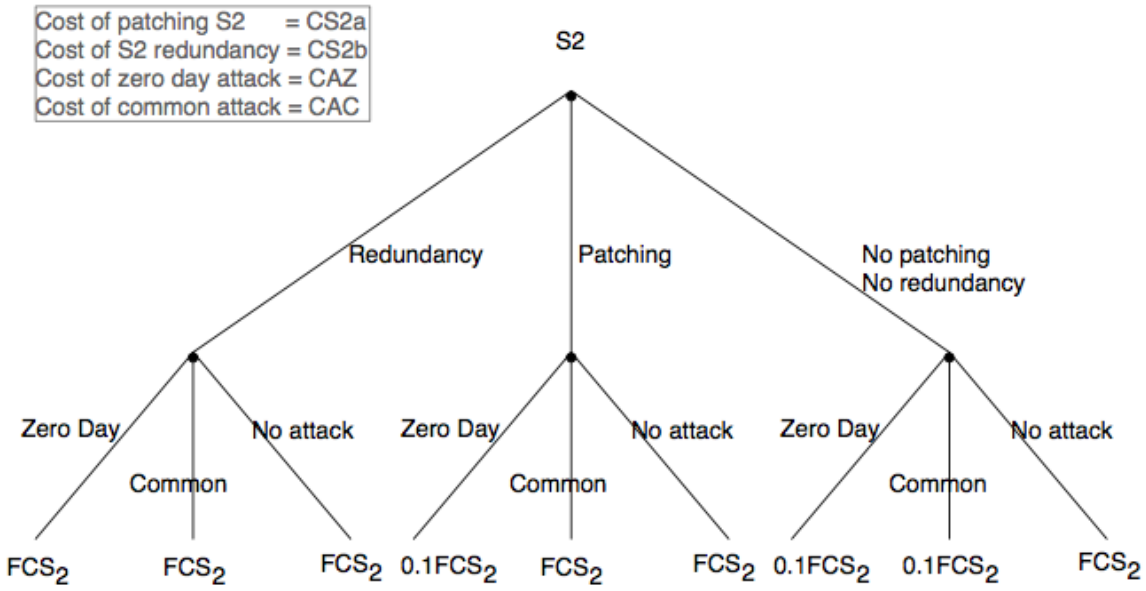


Figure 22: "Attack/Defence on S2" tree

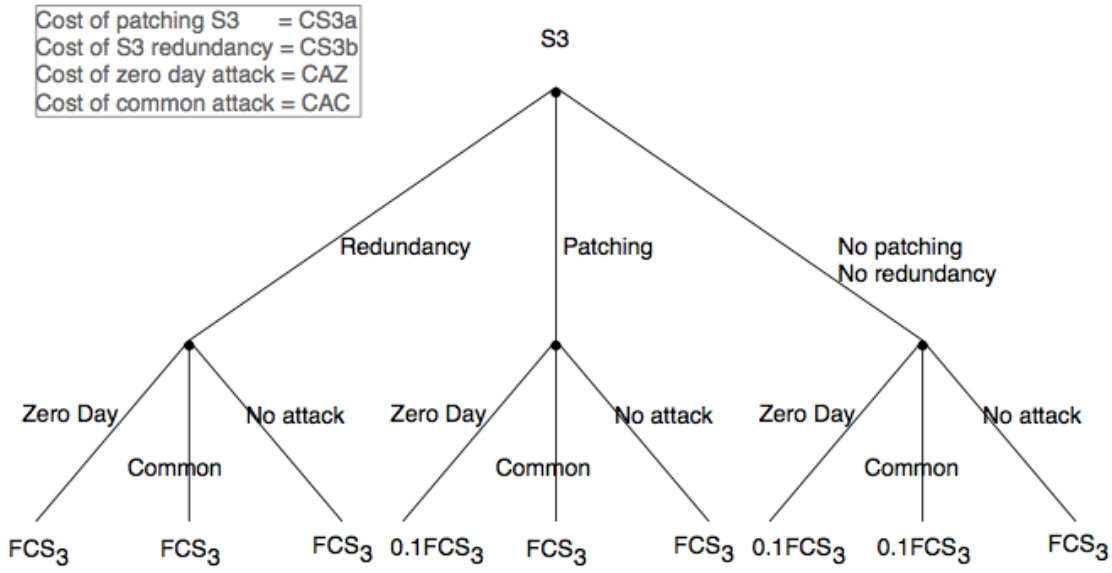


Figure 23: "Attack/Defence on S3" tree

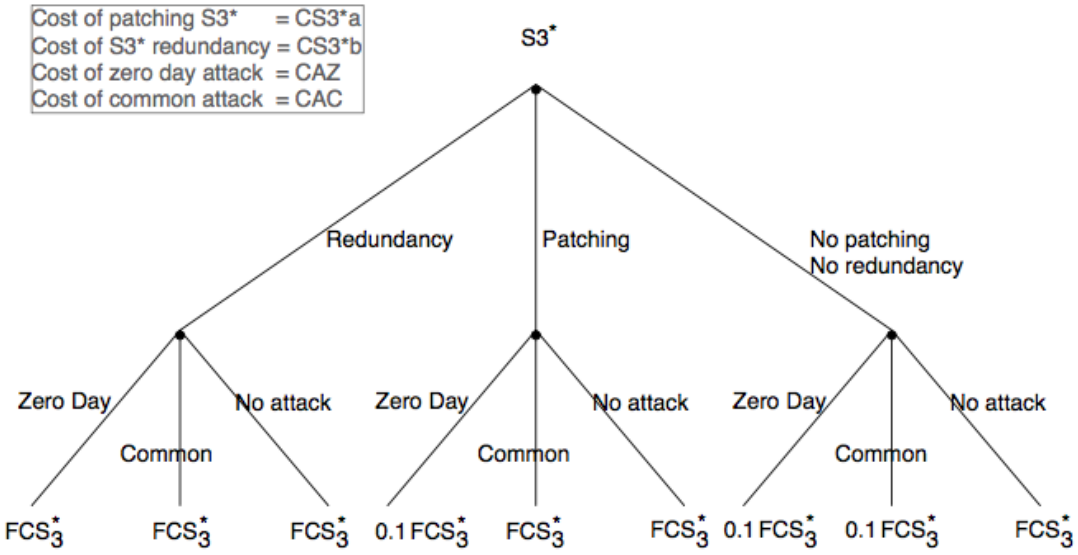


Figure 24: "Attack/Defence on S3∗" tree

Considering the game as a zero-sum game (since the defender's loss is the attacker's gain and vice versa), the players' payoffs are calculated as:

$$DPayoff = P'_{total} - DCost + ACost \tag{29}$$

And

$$APayoff = -DPayoff = -P'_{total} + DCost - ACost \tag{30}$$

where P'_{total} is calculated based on Equations (27) and (28) using the attack/defence trees, $DCost$ is the total cost of defence and $ACost$ is the total cost of attack.

Model Application – Case Study

In this section, we apply our model to the ICS of Figure 25. As shown, there are six elements to attack/defend, including the PLCs in the field level (that correspond to changes to the FCU_1, FCU_2 and FCU_3), the control server (FCS_2), the HMI ($FCS_3{}^*$) and the engineering workstations (FCS_3) within the control centre. The game revolves around

these elements and depends on the way their functionality changes as a result of the opponents' chosen strategies.

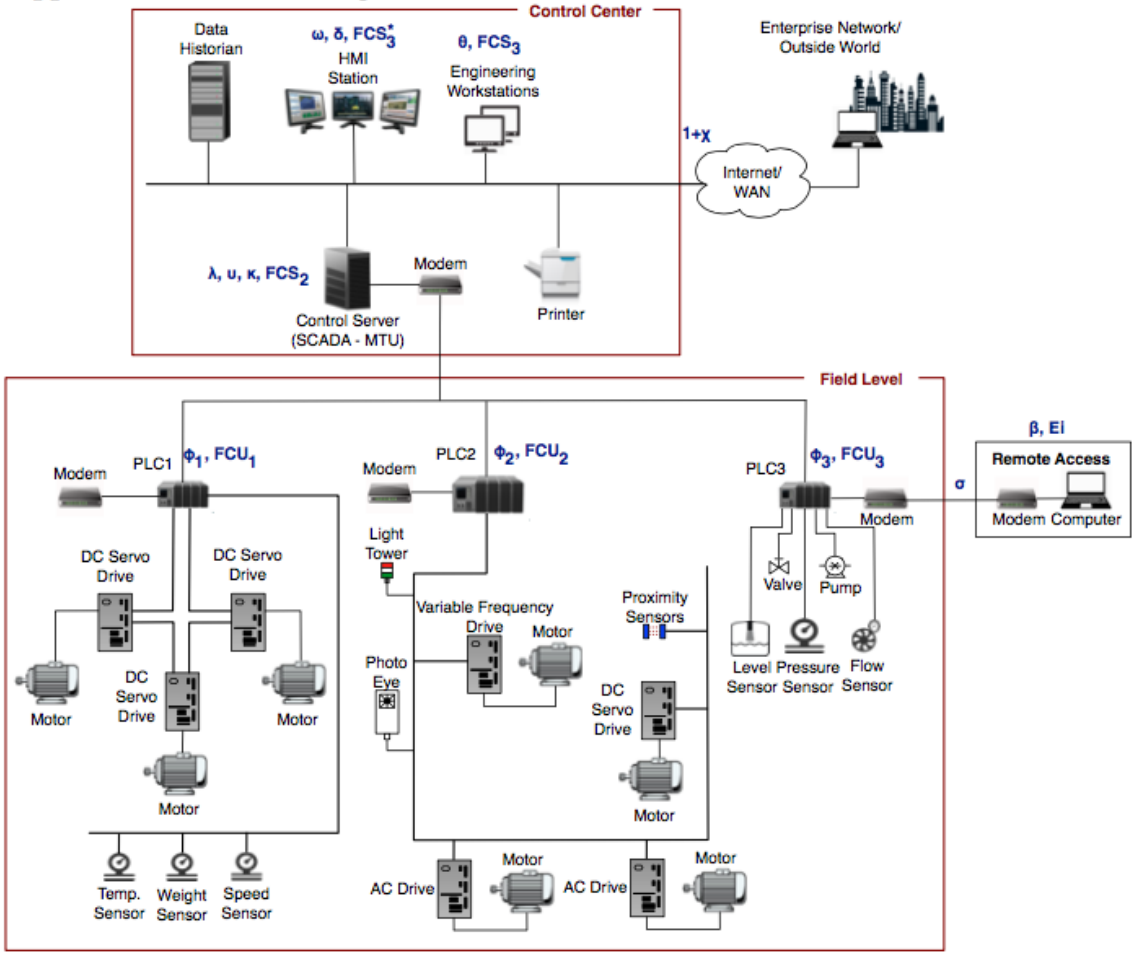


Figure 25: ICS Example

We consider that initially all elements operate in optimal performance (FCU_1= FCU_2= FCU_3= FCS_2= FCS_3* = FCS_3*= 100%). Additionally, we assume that the HMI (S_3*), the workstations (S_3) and the SCADA server (S_2) are equally important to the system ($\omega = \delta = \theta = \lambda = \upsilon = \kappa = \chi = 1$). Furthermore, since there is only one connection of the field level to the environment (remote access to PLC3) and is used for maintenance rather than control purposes we consider $\sigma = 0.5$ as the weight for the connection to the total environment and $\beta = 1$ as the weight to the remote connection in particular. For the purposes of our illustration we also assess the importance of the field level devices (PLC1, PLC2 and PLC3) based on the processes they control. In particular, PLC2 controls four

motors (the highest number of devices compared to the other PLCs), therefore we consider Φ_2 = 1. PLC1 controls three motors, thus Φ_1 = 0.9. Finally, since PLC3 controls only one process (the valve) we consider Φ_3 = 0.7.

In a real-world scenario, these values would derive from the asset evaluation process where the ICS operator would identify and assess all system assets.

The most challenging part of the model application is the cost evaluation. As we mentioned in the previous section, the available moves for the defender include patching, redundancy and "no security". The cost for the latter is DCost = 0. However, the cost for the patching and redundancy strategies is based on the ICS implementation and the operator's budget that are difficult to simulate. In our experiment we consider that the ICS operator uses legacy devices (PLCs) in the field level that are difficult to reboot or replace (in some cases legacy devices may not be available in the market) and modern machines within the control centre. Thus, the cost of patching or redundancy for the field-level elements is much higher than the cost of securing the elements within the control centre. Additionally, in a modern system it is easier to patch than deploy redundancy. In short, we assume the following values for the defender's costs:

- When deploying redundancy for elements within S_1(field-level elements): CS1b = 10^7.
- When patching elements within S_1 (field-level elements): CS1a = 10^5.
- When deploying redundancy for the HMI (S_3^*): CS3*b = 10^4.
- When patching the HMI (S_3^*): CS3*a = 10^3.
- When deploying redundancy for engineering workstations (S_3): CS3b = 10^4.
- When patching the engineering workstations (S_3): CS3a = 10^3.
- When deploying redundancy for the SCADA server (S_2): CS2b = 10^3.
- When patching the SCADA server (S_2): CS2a = 10^2.

From the attacker's point of view, we have only two costs, the cost of deploying a zero-day attack and the cost of deploying a common attack. We assume the following values for the attacker's costs:

- Cost of zero-day attack: CAZ = 10^5.
- Cost of common attack: CAC = 10^2.

Based on this information we can now construct the attack/defence trees in Figure 26, Figure 27, Figure 28, Figure 29, Figure 30 and Figure 31

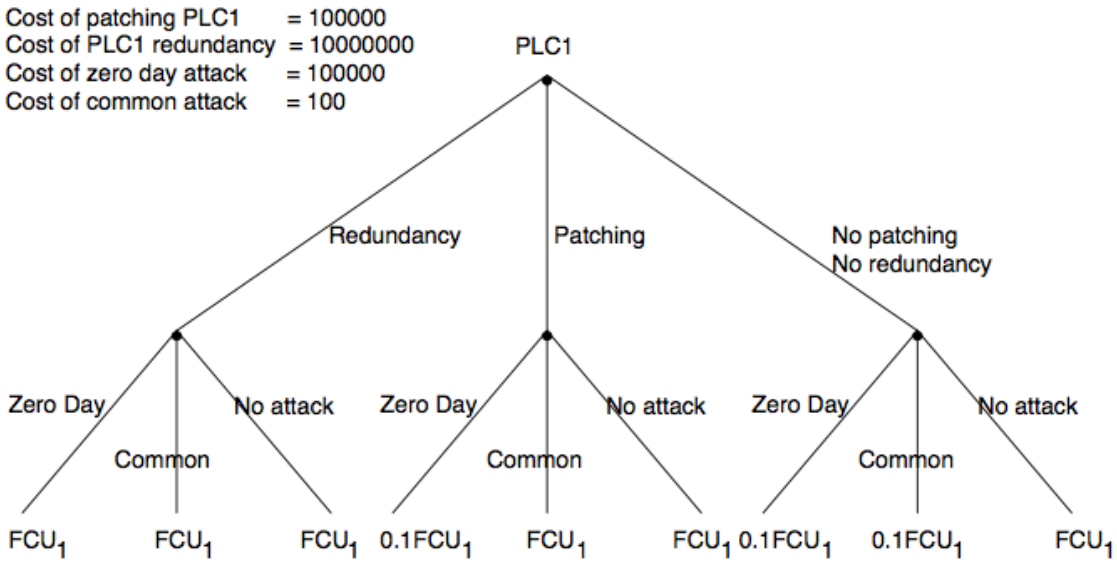


Figure 26: Attack/Defence tree for PLC1

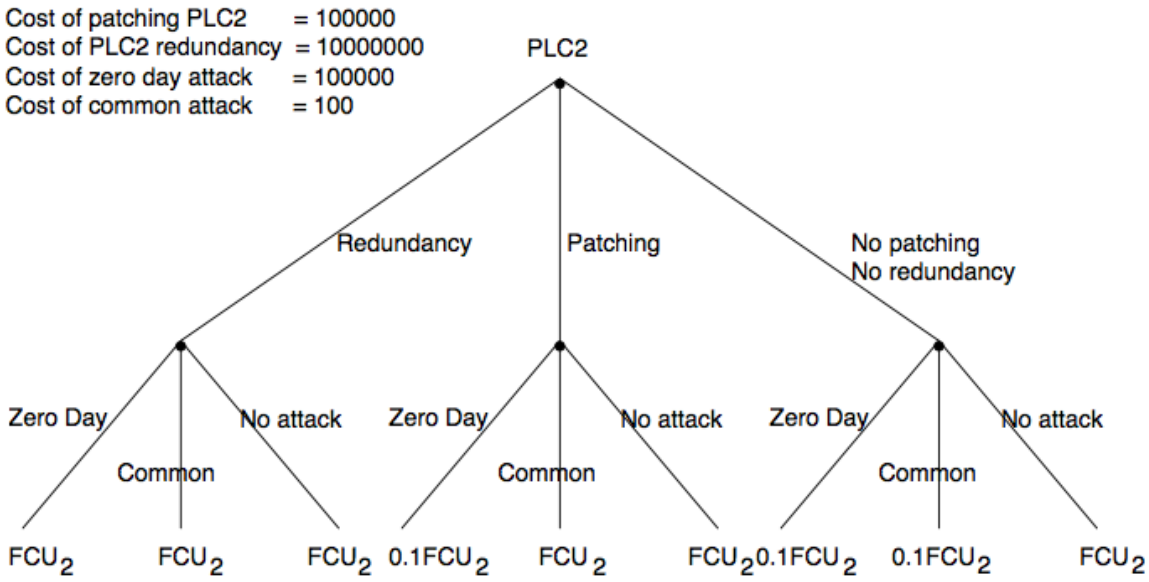


Figure 27: Attack/Defence tree for PLC2

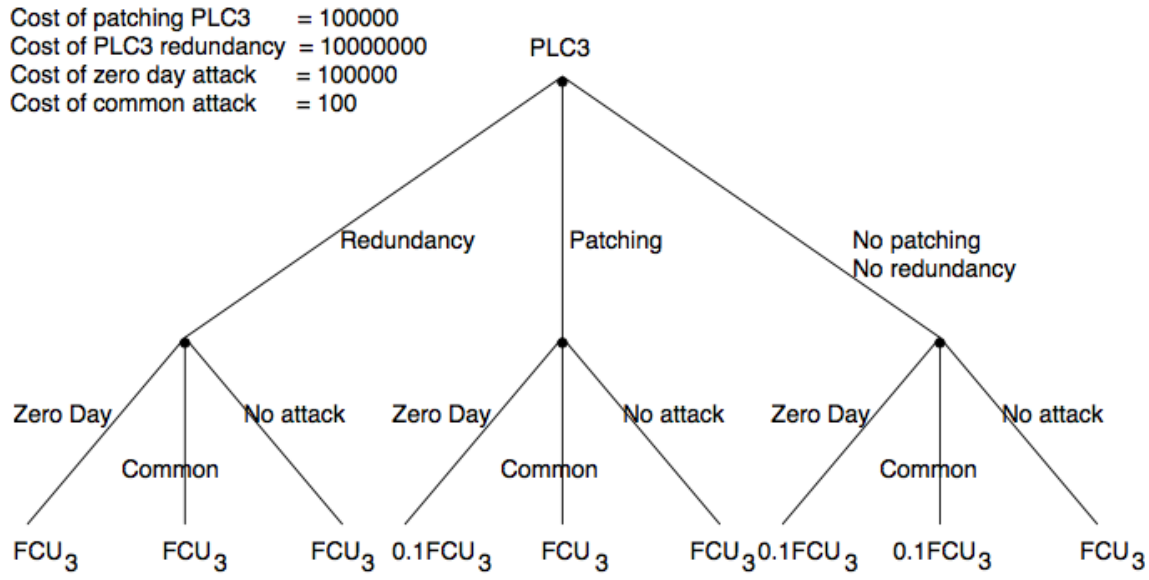


Figure 28: Attack/Defence tree for PLC2

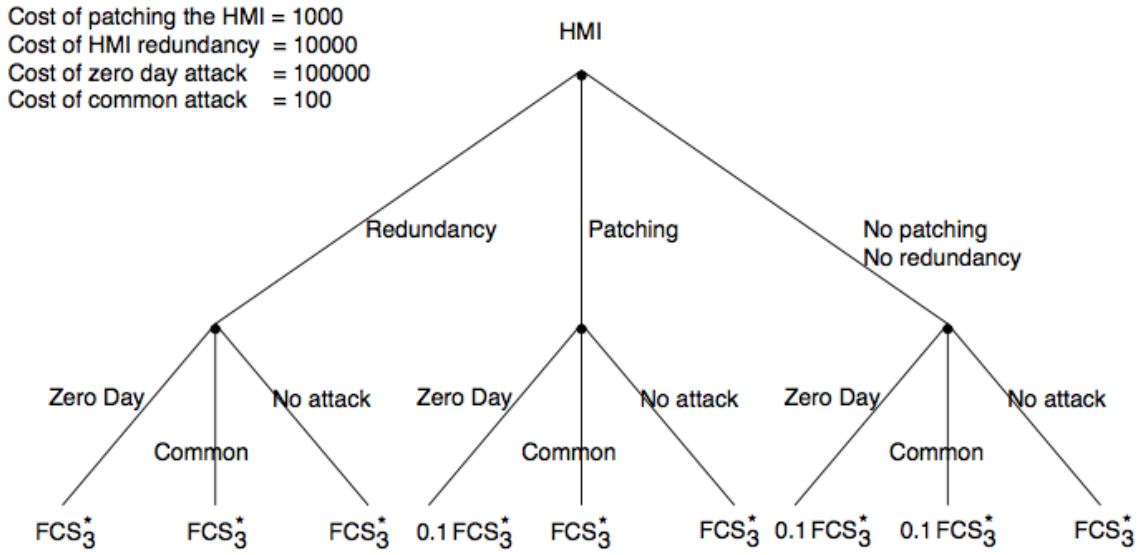


Figure 29: Attack/Defence tree for HMI

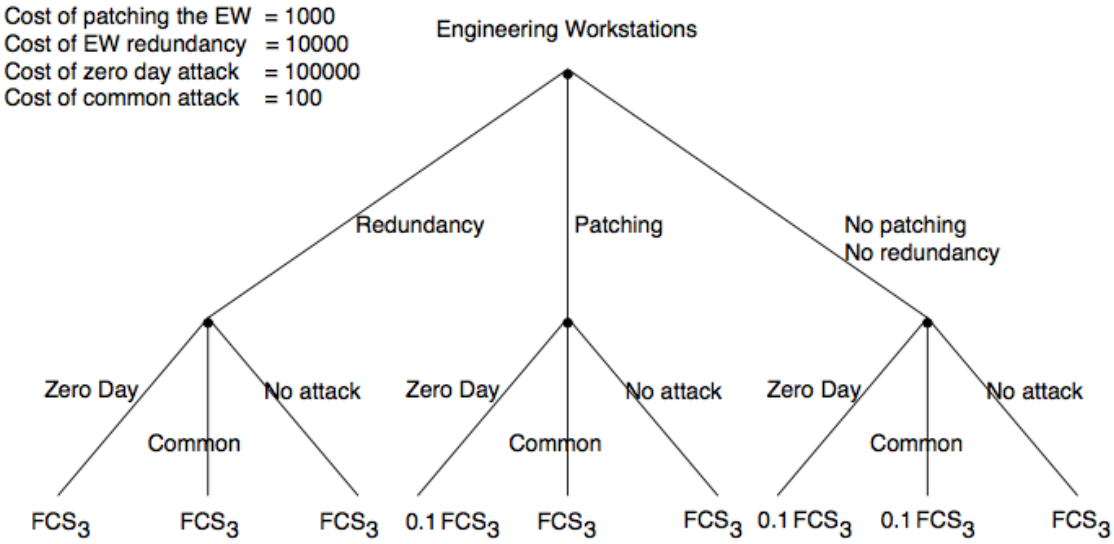


Figure 30: Attack/Defence tree for Engineering Workstations

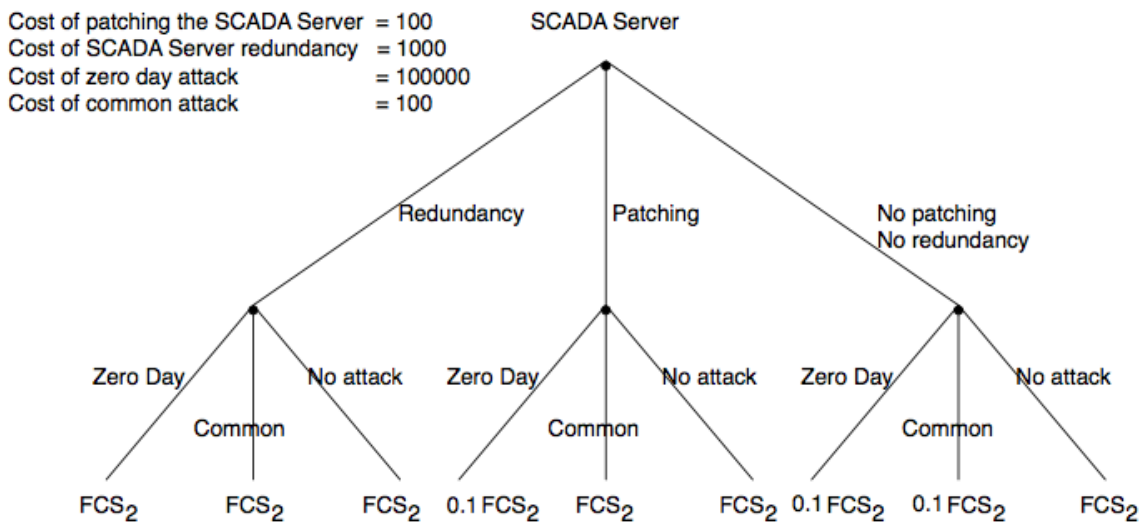


Figure 31: Attack/Defence tree for SCADA server

Based on the attack/defence trees we can identify all possible scenarios in the game. Since the defender can apply either patching, redundancy or "no security" to each of the six elements, the number of available defence strategies is 3^6. Additionally, since the attacker can choose between zero-day, common attack or "no attack" for each element, the total number of attack strategies is 3^6. Figure 32 shows part of all available pair of strategies along with the defender's corresponding payoff calculated based on Equation (29). In order to find the Nash Equilibria of the game, we apply the algorithm where the attacker tries to maximise her minimum payoff and the defender to minimise his maximum loss. The algorithm is also known as *low risk algorithm* and can be described with the following two steps:

- Defender calculates the minimum payoffs for each of his 3^6 strategies, based on the fact that for each of them, the attacker would choose a strategy that minimises defender's payoff (at the end of this step the defender has 3^6 minimums).
- Among those 3^6 minimums, the attacker chooses the strategy that returns the highest minimum payoff. This corresponds to the Nash Equilibrium in this case.

Figure 33 plots the minimum payoffs for each of the defender's strategies. As seen there are four areas that return maximum minimums. In particular, the defender's strategies that correspond to the Nash Equilibrium are:

- Strategy no.16: 000120 (patching S_2 and applying redundancy to S_3)
- Strategy no.93: 010102 (patching PLC2, patching S_2 and applying redundancy to ${S_3}^*$)
- Strategy no.257: 100111 (patching PLC1, patching S_2, patching S_3 and patching ${S_3}^*$)
- Strategy no.343: 110200 (patching PLC1, patching PLC2 and applying redundancy to S_3)

These are the optimal cost-efficient defence strategies.

Attacker's Strategies						Defender's Strategies						Payoff
0	0	0	0	0	0	0	0	0	0	0	0	7.29E+41
0	0	0	0	0	0	0	0	0	0	0	1	2.7E+14
0	0	0	0	0	0	0	0	0	0	0	2	2.7E+14
0	0	0	0	0	0	0	0	0	0	1	0	2.7E+14
.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.
0	0	0	0	0	1	0	1	0	0	2	2	-115398
0	0	0	0	0	1	0	1	0	1	0	0	-95499
0	0	0	0	0	1	0	1	0	1	0	1	-96498
0	0	0	0	0	1	0	1	0	1	0	2	-105498
.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.
1	2	1	2	1	1	1	2	0	0	0	0	-9899604
1	2	1	2	1	1	1	2	0	0	0	1	-9900603
1	2	1	2	1	1	1	2	0	0	0	2	-9909603
1	2	1	2	1	1	1	2	0	0	1	0	-9900603
.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.	.	.
2	2	2	2	2	2	2	2	2	2	1	2	-29412000
2	2	2	2	2	2	2	2	2	2	2	0	-29411001
2	2	2	2	2	2	2	2	2	2	2	1	-29412000
2	2	2	2	2	2	2	2	2	2	2	2	-29421000

0 -> 'no attack'
1 -> common attack
2 -> zero-day attack

0 -> 'no defence'
1 -> patching
2 -> redundancy

Figure 32: Available strategies

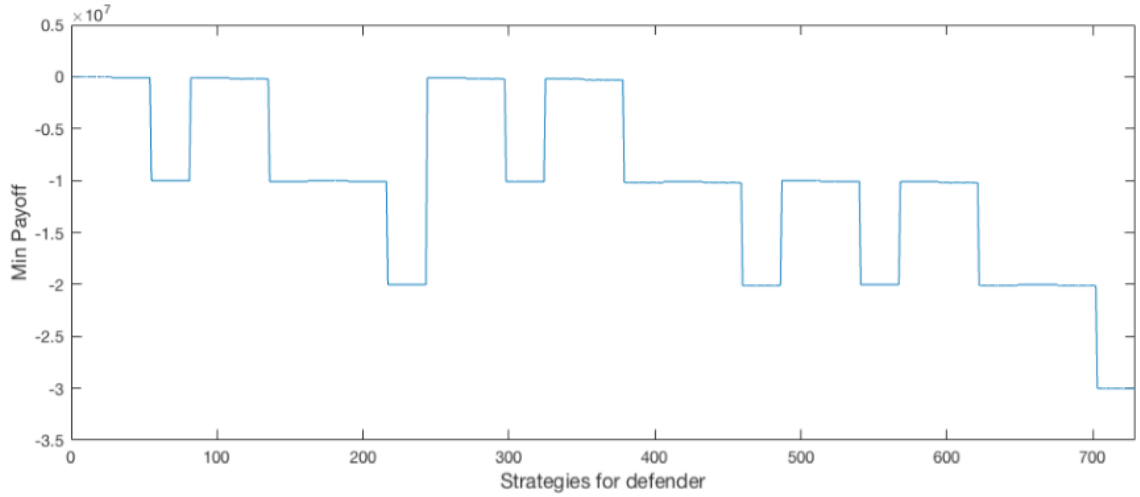


Figure 33: Defender's minimum payoffs for each of her strategies

Findings and Conclusions

In this work, we combined two classic Systems Analysis techniques, VSM and Game Theory, in order to model an ICS through a living analogy. Unlike the traditional risk analysis methods, where emphasis is on calculating probabilistic measures of risk based on perceived likelihoods of threat occurrences, our approach allowed us to compose a set of formulae that describe the level of service provision of an ICS and can provide the basis for an impact analysis through the lenses of viability (defined the ability to maintain a core level of functionality, as it would deem necessary per critical infrastructure). Based on the perceived significance of interacting components and an estimate of the impact of their compromise we set up typical scenarios of attack and defence in ICSs as games between rational players and compute Nash Equilibria for varying strategies of redundancy and immunisation. This approach can be used to design defences against unknown attacks, with reference to the system architecture only.

3.3.2 CI-ICSs Risk Management using Monte Carlo Predictive Modelling

The content of this section addresses part of RQ2 by expanding on our Monte Carlo predicting modelling which can serve as a benchmark for policy and decision support to aid stakeholders in optimizing resource allocation for cyber security investments.

There are a lot of fundamental issues associated with risk evaluation, reporting and mitigation costs in the IT security domain. The problem of cyber security risks management in corporate organisations is non-trivial, hence, constructing tools that truly satisfy risk measurement theory is difficult and not readily available [136]. Information security is fundamentally concerned with the confidentiality, integrity and availability of information assets at all times. In order to defend against threats to information assets, organisations invest in countermeasures. However, as the number of assets to be protected grows and IT budgets are constrained, there is need for deliberate evaluation of information security investments [137]. Cyber security is one of the biggest challenges that businesses face today. Economic loss due to cyber-attacks is on the increase and many businesses have been obliterated due to the loss of intellectual assets to cyber criminals. This figure is set to grow exponentially, according to the study conducted in [138] which enunciated that by 2020, losses from cyber-attacks may hit the $20 trillion mark. In a different report [139], studies conducted to quantify the actual and potential value of losses as a result of successful system breaches is placed in the region of $500 million and $5 billion per year in the United States alone. Hence, the importance of risk management cannot be over-emphasised. As firms' vulnerability to cyber-attacks increases, so is the need for further investment in enhancement measures. Security managers can effectively reduce the potential and probability of loss to cyber rouges by reinforcing firms' cyber capabilities. [140].

What constitutes Information Security risk, is relative to organization risk acceptance level. However, in all cases, security managers' priority is to mitigate organizational risk exposure that could undermine the confidentiality, integrity and availability of mission-critical systems. Apart from huge financial losses, security breach can lead to sanctions from industry regulators, negative corporate image, and loss of

confidence in clients and customers. A classic example is the case of TalkTalk, a UK giant communication firm that was hacked in 2015. Personal details of nearly 157,000 TalkTalk customers were accessed through a rudimentary SQL Injection attack on the company's website. More than 15,000 personal account numbers and sort codes were also stolen. Impact of the cyber-attack is reported [141][142] to have cost the company £42m, loss of over 100,000 customers and a fine of £400,000 for data breach by the Information Commission Office (ICO). The ICO claimed that hacks could have been prevented if TalkTalk had implemented basic cyber security measures to safeguard its customers' data.

Taking into consideration the aforementioned facts, this work explores how Monte Carlo simulation model can be used for effective cyber security resource allocation and investigates how to make a business case for resource allocation decisions within an enterprise or Small and Medium-sized Businesses (SMBs). Monte Carlo simulations have been extensively used by risk analysts in various fields of study to make future risk estimations [143]. A simulation approach to managing and visualising uncertainties in cyber-security context allows different variables to be applied to different risk scenarios, for optimal resource allocation to mitigate and manage those risks. Monte Carlo simulation can perform quantitative risk analysis by assigning probability distribution to uncertain parameters; and through random sampling of the distribution, it is possible to determine all potential outcomes under those uncertainties [144].

Risk Management Overview

Information security risks are generally described under the broad categorization of disaster or abuse. Top priority of Chief Information Officers (CIOs) and management is to ensure continual functionality of IT resources at all levels of operations. Risk management can be described as a systematic and logical approach for identifying, treating, analysing and monitoring risks in any process. Managers benefit from risk management strategies as it has direct bearing on how available resources are put to best use. Risk management is practiced in both private and public sectors; including health care, government establishments, insurance, finance and investments. However, in the context of Information Security, risk management is about the protection of information

assets. Information Security Risk Management is defined [145] as the protection of information assets from a wide range of threats in order to ensure business continuity, manage business risk and maximise return on investment. Risk management within the context of an organisation involves the implementation of appropriate controls to mitigate, share, transfer, insure, accept and continually manage risks as set out in the ISO/IEC 27001:2013 (2014) Standard. The ISO/IEC2700 series of standards define best practices, baseline requirements and controls for information security management systems (ISMS), under the confidentiality, integrity and availability (CIA) triad. In addition, given that threat climate changes all the time, it is essential that the effectiveness of security controls be periodically reappraised by the organization. This is an important element of risk management cycle [146]. There are various reasons why an organization may require some measures of security control against potential threats; these could stem from internal factors like corporate regulations and organizational policies, or mandatory external influences like the data protection acts or compliance requirements of industry regulators. Whatever the driver, it is apparent that risk management will involve some mitigation control investments and resource allocation decisions.

However, Information Security professionals often do not quantify and communicate risks effectively in order to attract the right level of resource allocation. Again, organisations may struggle to present a measure of accurate cost benefits of information security activities, primarily because security investment results in loss prevention rather than profit margins [147]. That is why business executives often opt for compliant security, whereby, baseline requirements of standards like the ISO2700, NIST etc. are implemented, then businesses operate under the assumption that compliance equates security. Whereas, this is often not the case because baseline controls may be enough for industry regulators and business executives but often fail to result in holistic protection [148]. The costs associated with risk management range from personnel to hardware and software outgoings. Therefore, information security expenditure is a crucial resource allocation decision, yet little is known about the budgeting process used to ensure optimal investment in information security capabilities [149], or at best, the budgeting process is generally beclouded with ambiguities.

Traditionally, organisations use risk assessment model to determine the optimal allocation of resources to cyber capabilities. This approach is a flavour of risk-based

regulation whereby firms determine their security investment based on risk-assessment analysis, potential losses and investment profile [150]. An organisation's budgetary decision is then based on its threat tolerance and its score from the risk scoring matrix. Risk scoring matrix is calculated on the assumption that an event will happen given a probability of occurrence, and impact or severity of security breaches. Information security budget is then allocated based on the resultant estimated risk score. The risk scoring formula is given as:

$$Risk = Probability(P) \times Impact\ (I) \tag{31}$$

Values of (P) and (I) for a given asset are assigned based on expert opinion and their product represents the risk score for that particular asset. To suggest that the risk and impact of threat to information assets are subjective probability estimates is rather ambiguous and deterministic. In practice, it is difficult to apply this calculation to real world problems, in order to optimise resource allocation decisions. This approach raises the question of reliability [27], as risk predictions are misrepresented for effective mitigation. Information security risk and management is transitory, hence, actual impact of risky events might not be a true reflection of the current deterministic estimation.

Different Approaches to Resource Allocation Decision Processes

When risk analysis is based on the traditional risk matrix approach, security assessors extrapolate that under certain assumptions, certain events would be true; while completely discarding the possibility of least significant and extreme events as part of that extrapolation. For organisations that base their threat tolerance on information security risk assessment, trying to guess the odd under so many uncertainties can only lead to erroneous results. Difficulty of this approach is further emphasised in [151], where it is stated that effective allocation of resources under the circumstance of uncertain risk and severity of breach cost is very hard. In order to explain how uncertainty affects security breach costs and resource allocation decision to mitigate those risks, we present a conceptual enterprise scenario for a bank in Figure 34 and Figure 35.

Figure 34: High level conceptual model diagram

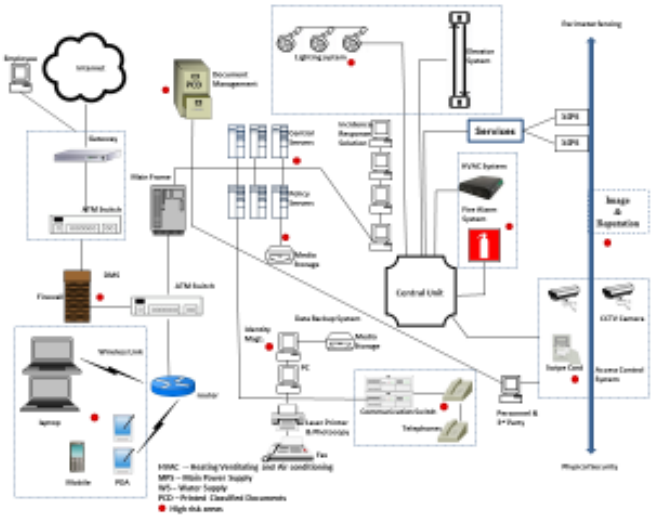


Figure 35: Low level conceptual model diagram

We assume that the bank has only 5 high risk asset points that need to be safeguarded from security threats at all times. Also, stakeholders' resource allocation decision is based on the severity of breach to those assets and how it may impact banking operation. For illustrative purposes, we consider (DDoS) Mitigation System, Personnel and third-party contractors, Data Backup and Recovery System, Incident Response Solution, and Antivirus Software as the key assets or factors.

Deterministic Estimation of Security Breach Costs

Below we elaborate on both the deterministic and the probabilistic estimation of the security breach costs.

The deterministic approach is based on the use of conventional risk assessment model to determine appropriate resource allocation. Deterministic point estimation is associated with random variability like a game of chance. In a roll of die, probabilistically, there is a 1/6 chance that a certain number would come up, and it would have an interpretation given long-term frequency. Risk/vulnerability output is based on a five-level scale (very low, low, medium, high and very high) and it similarly has five probability levels. See Table 6 for description of likelihood and severity of risk, especially in terms of financial impact. Likelihood of risk is ranked on the scale of 1 to 5 where 1 is rare or very low and 5 is frequent or very high.

Table 6: Risk likelihood and severity description

Likelihood	*Description*	*Frequency of occurrences*
1	An incident is expected to occur in exceptional circumstances, e.g., once in 10 years.	Rare/very low
2	An incident may occur at some point, e.g., once in 3 years.	Possible/low
3	An incident will occasionally recur, e.g., once in a year.	Probable/medium
4	An incident will occur in most circumstances, e.g., once every 4 months.	Certain/high
5	An incident is certain to occur in most circumstances, e.g., once every month.	Frequent/very high
Severity	*Description*	*Example of business impact*
1	None: no disruption of service	Financial loss < £1,000
2	Minor	Financial loss < £10,000
5	Moderate	Financial loss < £100,000
10	Significant	Financial loss < £1,000,000
15	High	Financial loss > £1,000,000

Similarly, Table 7 shows the risk scoring matrix by taking into account the likelihood and severity value of each risk. Risk scoring is carried out by applying a simple multiplication process whereby the likelihood of risk is multiplied by the severity of that

risk occurring. After scoring each risk, risk rating is then applied by choosing the most appropriate definition under likelihood and the most appropriate definition under severity, then the numbers are looked up on the risk matrix table and matched to obtain the risk rating. After the risk analysis phase, given an organisation risk threshold and the risk score, budget is allocated for countermeasures to mitigate risks in that context.

The idea of risk assessment is to evaluate scenarios of security incidents and take proactive measures before it happens. Consider one of our scenario high risk assets; a dedicated DDoS Mitigation System (DMS) that can deter DDoS attacks. How effective the DMS is to mitigate volumetric attacks may be uncertain but it is unlikely that an enterprise operations and vital computing resources will be subjected to complex layer 7 attacks, in order to ascertain if the defence mechanism is worthy of investment. Rather, it is more likely that we use historical data to assist with resource allocation decisions, but in the absence of data we can use estimations. A risk analyst may make a statement that the probability of a successful attack without mitigation (the DMS) is 3, and the cost impact in terms of human and financial resources needed to recover from the attack is $53,477.

Table 7: Risk rating table

Severity →		*None*	*Minor*	*Moderate*	*Significant*	*High*
Likehood ↓		*1*	*2*	*3*	*4*	*5*
Frequent	1	5	10	25	50	75
Certain	2	4	8	20	40	60
Probable	3	3	6	15	30	45
Possible	4	2	4	10	20	30
Rare	5	1	2	5	10	15

However, when deterministic point estimate is used to score risk and model uncertainties; what that actually means is that based on the subjective estimates for each asset point, the total breach cost without security investment for all tangible and intangible assets in the enterprise, will always be the sum of breach costs to each asset (as shown in Table 8). If it is certain that an expert's deterministic estimate is 100% reliable, then potential security breach costs should be fine, hence resource allocation to mitigate those

risks should correctly reflect the assessment. In reality, a security breach to some asset will cost less with insignificant impact while some may result in colossal losses with catastrophic consequences. Therefore, resource allocation under uncertain risk-based assessment is unlikely to match risk mitigation efforts.

Table 8: Expert estimation of security breach costs

Average annual cost of security breach in magnitude of $K/year		
Assets	*Security incidents*	*C = Cost of breach*
DMS	DDoS attack	53,477
Personnel and 3rd party	Malicious insider	40,403
Recovery system	Data loss	39,905
Incidence response	Cyber espionage	69,026
Anti-virus software	Malicious code infection	31,572
	Total	234,383

Probabilistic Estimation of Security Breach Costs

In order to address the huge amount of uncertainties associated with deterministic approach, especially in view of increasing information assets; we can consider the probabilistic approach. Through Monte Carlo simulations, we can determine the probabilistic cost of breach for each asset in a given scenario. The Monte Carlo simulation works by sampling lots of scenarios from a probability distribution instead of static point estimates. Probabilistic estimation assigns minimum and maximum cost boundaries for each security breach. The combined cost of all security breaches is then calculated as the total minimum and maximum cost of a security breach for each asset in order to project total resource allocation for the enterprise. In that case, it is possible to establish absolute bounds for allocated resources to the entire enterprise.

Monte Carlo may not be able to tell with certainty the exact cost of breach, but it can describe the probability of cost associated with security breaches, to aid resource allocation. In comparison to the deterministic approach, probabilistic estimate is also based on random variable, however, each estimate follows a particular distribution, independent and unaffected by other variables.

Table 9: Model simulation parameters

Assets	*Security incidents*	*Unit cost of security breach without risk mitigation investments (in magnitude of $K/year)*		
		C_{min} = *minimum*	C_{ml} = *most likely*	C_{max} = *maximum*
DDoS mitigation system	Dos/DDoS attack	30,000	53,477	65,000
Personnel and third party contractors	Fraud/malicious insider	20,000	40,403	50,000
Data backup and recovery system	Data loss/stolen devices	25,000	39,905	45,000
Incident response solution	Cyber espionage	35,000	69,026	75,000
Antivirus software	Malicious code infection	15,000	31,572	37,000
Total		123,000	234,383	272,000

We will now consider the deterministic cost of breach for the DMS as described in the previous section. Under probabilistic estimation approach, we can use a smearing out parameter to suggest that in place of a fixed quantity like $53,477, we could include minimum value in of $30,000 and the maximum value of $65,000 in a distribution, as shown in Table 9. Essentially, we replace a fixed value with probability distribution, which is a true representation of state in the real world. Hence, the fixed quantity is now our most likely value, but it is not the only possible value in the distribution. The key to Monte Carlo simulation is that, each variable is assigned a random value; and the total value is calculated thousands of times during the simulation. It therefore allows us to understand the risk that expectations may not match reality, hence, appropriate precautions can be taken [152]. It is difficult to compute values for multiple scenarios without some form of simulation, especially if we have to factor-in multiple assets and security breach costs, as part of the budgetary allocation process.

Methodology

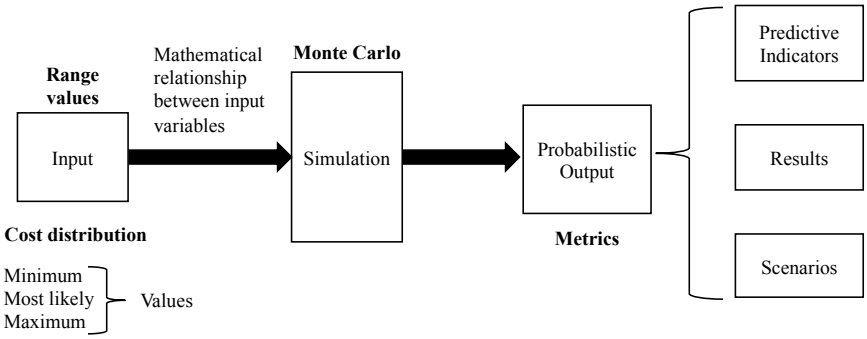
There are two basic assumptions for this model:

- Key information asset points are determined by an organisation CIO and the security team.
- Minimum and maximum values of security breach costs are subject to expert elicitation, based on experience and previous security breach events.

The work described in this paper uses some security breach cost parametric values obtained from verifiable information security breach reports. Model parameters are taken from the Ponemon Institute 2015 cost of security breach report [153] and Kaspersky Lab IT security risks special report series [154]. The study in [153] covered data breach cost and impact of 350 organisations around the globe. The study uses Activity-Based Costing (ABC) for data breach calculation which takes into account the direct cost, the indirect cost and the opportunity cost. It also takes into account a range of expenditure associated with organisation data breach detection, containment, response and remediation. The study in [154] covers corporate IT security risks survey of more than 5500 companies in 26 countries around the world. It covers IT threats and the cost of recovery when security breach occurs. Values taken from both studies serve as input parameters for our simulation model as shown in Table 9. However, limitations of the costing methodology outlined in the studies are not validated nor described in this work.

We identify uncertain deterministic security breach costs in our model and convert them into ranges using a triangle distribution, as shown in Figure 37. Each asset's breach cost estimated fixed values are replaced with a probability distribution. Triangular distribution used in this model, is one of the most used probability distributions to elicit expert opinion, especially in the case of limited or absence of historical data. It defines uncertain breach cost values as minimum (C_{min}), most-likely (C_{ml}) and maximum (C_{max}) range of values, for each asset in the model calculations.

Table 10: Schema of the Monte Carlo predictive model



This approach shares some similarities with the model implemented in [155], whereby the (C_{min}) and (C_{max}) are held constant while the values of (C_{ml}) are selected randomly from the distribution graph. (C_{ml}) is a non-negative random variable which follows a triangle distribution. For this simulation, we used MATLAB and Vose ModelRisk software [156]. Both tools allow configurable simulations with a very large number of runs and can generate thousands of scenarios for each set of uncertain inputs. ModelRisk uses a mathematical model for input variables and triangle distribution function given as:

$$f(x) = \frac{2(x - C_{min})}{(C_{ml} - C_{min})(C_{max} - C_{min})} \; for \; C_{min} \leq x \leq C_{ml} \tag{32}$$

$$f(x) = \frac{2(C_{max} - x)}{(C_{max} - C_{ml})(C_{max} - C_{min})} \; for \; C_{ml} \leq x \leq C_{max} \tag{33}$$

Simulated output is generated given the mathematical relationship with input variables, and the results provide predictive indicators to support decision making processes. However, with Monte Carlo, input variables for the simulation model are uncertain, random and defined according to a probability distribution in order to capture and model those uncertainties. In this model, what happens is that thousands of scenarios are generated to reflect a probabilistic output for each uncertain input, according to triangle distribution, then, the resultant output values are computed thousands of times

over again during the simulation. However, in order to obtain a convergence and more realistic values, a recommended run of 10,000 simulations is required, with 1,000 of them being the barest minimum acceptable [157]. We generate 50,000 simulation runs; the model output is a probabilistic range of values and scenarios associated with security breach costs, as well as the probability distribution associated with those values.

Results and Findings

Results of Monte Carlo simulation shown in Figure 36 add extra dimension to the initial deterministic values. As the simulation begins, sample is taken from each of the breach cost probability distribution. ModelRisk then computes the average random value at the end of each iteration. During the simulation, different scenarios are generated based on the frequency proportional to the probability of it occurring.

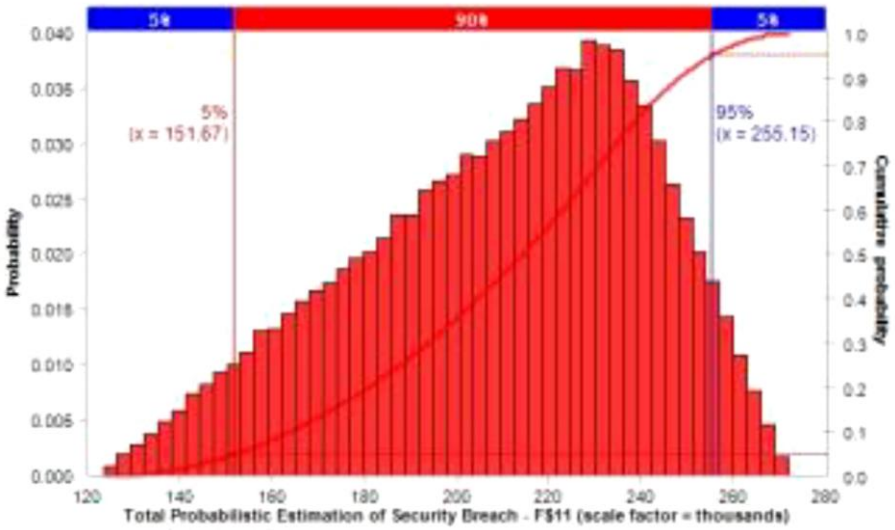


Figure 36: Simulation result with cumulative overlay

At the end of the simulation, the output histogram represents 50,000 scenarios for security breach cost. Result of the simulation takes into account all uncertainties and it is in the form of probability distribution similar to the input parameters. These distributions represent possible outcomes, rather than single point predicted outcome.

From the model result in Figure 36, it can be seen that the upper 5% and the lower 5% represents extreme cases that are marked differently by the simulation output because they are practically ignored. From the parametric values in Table 10, it can be seen that the total resource allocation could be as low as $123K or as high as $272K, but the realistic chance of resource allocation nearing these extreme values is very unlikely, hence the model ignored them. It can be seen that 90% of the simulation iterations fall under a value less than the upper bound estimated total values. Hence, we can say that 90% of the total allocation will meet our initial estimate. While this is not a guarantee, it allows us to adjust IT security budget to match cost of potential breaches and also understand the risk that resource allocation may not meet initial estimates.

Further analysis of the result in Figure 36 shows that given all iterations of simulation, the absolute minimum value of $151.67k is much higher than the original deterministic lower bound value of $123k. Similarly, the absolute maximum probabilistic value of $255.15k is much lower than the deterministic value of $272k, after iteration, with only 5% chance of the allocation going over this value. The most likely point estimate is around the value of $229k. From the location of the peak of the distribution, it can be seen that this value is rather more realistic than the deterministic value of 234,383. However, the cost of impact could be significantly higher, possibly twice as high in terms of cumulative percentage.

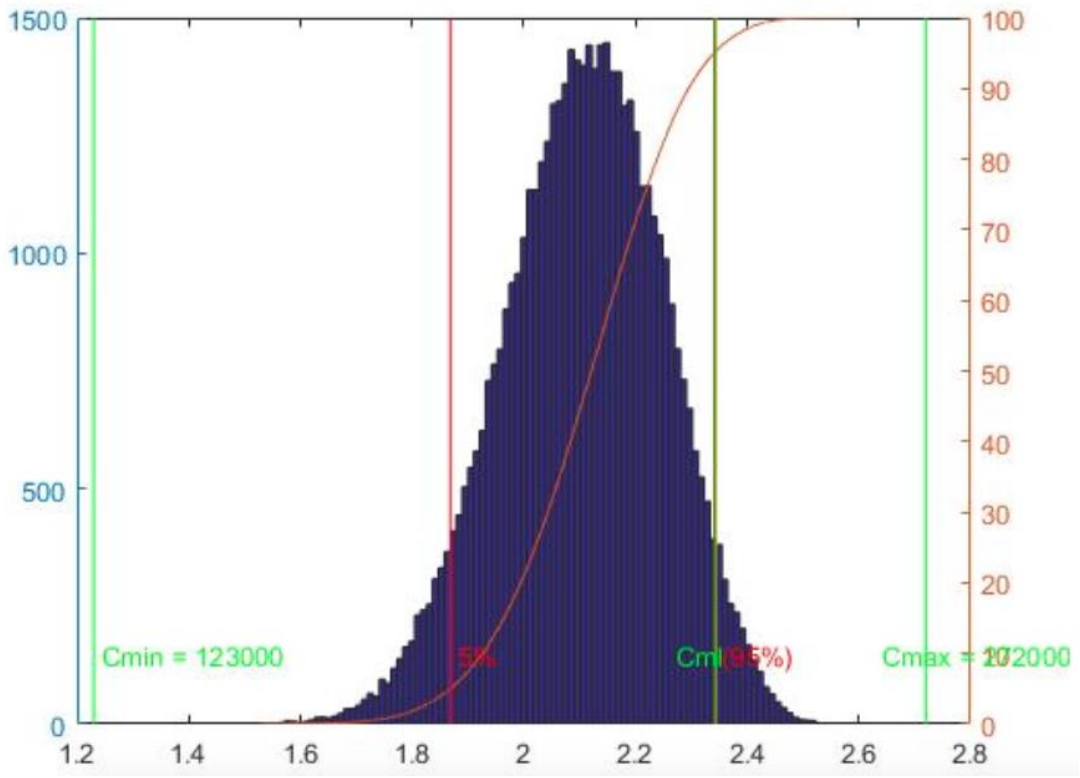


Figure 37: Simulation result in MATLAB showing values for Cmin and Cmax

In an attempt to validate our model, we compared the result with another simulation in MATLAB shown in Figure 37, using the same input parametric values. What is common in both states of the models is that extreme values are ignored in the output of both simulations. While both models follow similar distributions, it can be seen that not only did both simulations ignore lower and upper bound values, but also show higher $Cmin$ and lower $Cmax$ than the deterministic values. This is an additional reassurance about the validity of the representation entities behaviour.

Findings and Conclusions

In general, predictive models allow us to make more useful and less erroneous decisions. Making important decisions without diligent consideration to uncertainties in the budgeting process can lead to unrealistic values. Forecasting with accuracy, how much damage a successful security breach can cause is a real challenge for risk managers, especially when there are multiple assets and associated threat exposure. Traditionally

conducted estimates for all assets tend to become unreliable, especially, as the complexity of asset classes in the model increases. Using probabilistic simulation therefore simplifies the complexity of cost estimation processes. The application of Monte Carlo simulation to information security investment decision, in particular, allows us to visualize different probabilistic outcomes in view of what might go wrong; given best case, worst case and most likely case scenarios.

Monte Carlo also allows us to understand the outcome of scenarios and help to understand unexpected pattern or behaviour without necessarily exposing information assets to real threats. Output of Monte Carlo simulation is a range of values and risk assessor can derive confidence level from that range. It is expected that predictive models will enable management to make more effective decisions and be part of analytical input for policy formation If there is sound understanding of what might go wrong, decision makers can utilise the model to implements appropriate risk mitigation strategies and budget allocation for security investment.

This study can be expanded as part of future work to include different resource allocation patterns for different assets, depending on their characteristics. As such, assets with the highest frequency and impact of threat events could be allocated more resources than low impact ones.

3.3.3 Epidemiology

This section is about the use of epidemiology properties in order to build a custom-made epidemiology model, that borrows some features from the already established ones (SIR and SIS), in an attempt to provide a novel method for malware dissemination prevention.

3.3.3.1 Introduction

In order to face the spread of malware in a corporate network (S_4) we model its dynamics within the network resulting in finding ways to mitigate it in a cost-efficient way. Although there are other models in the literature that examine the dynamics of malware proliferation within a network, they are usually based on the traditional

epidemiological models (SIR and SIS), which were designed to describe the dynamics within human population. In addition, Game Theory is a very effective tool in situations where antagonistic interests are involved and has been introduced in the past in problems from the field of network security [2][158] where an attacker and a defender were interacting; the former aiming to harm the network and the latter aiming to keep it safe. Approaching malware as a threat agent is a reasonable assumption since its acts are based on inscribed behaviour that is coded by cybercriminals.

This work's aim is to combine epidemiology and a game-theoretic framework in order to describe a game between an attacker (malware) and a defender, each with their own set of strategies, trying to achieve their highest possible individual benefit. As a result of the game (during which we are taking into account the malware's spread dynamics as well) the defender is able to identify his optimal strategy while minimizing the security cost, on a cost-benefit basis.

3.3.3.2 Proposed Model

The content of this section addresses part of RQ2 by expanding on our approach that combines Game Theory and a custom Epidemiology model based on the traditional SIR and SIS ones, in order to provide a cost-benefit risk management framework for managing malware spread in computer networks.

Worms have the ability to self-replicate and spread without human intervention in a network [159], resembling human viruses. They may utilise various proliferation mechanisms, depending on the way they scan the network to find their new targets. Our work focuses on the examination of random scanning worms, which select their target IP addresses randomly without any topological restrictions [160][161]. For a random scanning worm, the whole Internet is seen as a fully interconnected network. Consequently, each node has the same probability to get infected. This type of malware has been widely used by cyber-criminals, since it is easy to deploy. However, such attacks have lower infection rates than other topology-oriented scanning methods, such as malware that spreads through email exchange or the social media. This holds true as, their

randomly picked IP addresses might not be used by any device. It is important to note that this work does not focus on modelling the malware dissemination process itself, instead it utilises already known modelling techniques and combines them with game theory in order to propose optimal mitigation strategies for the defender.

In the human virus spread paradigm, a "random scanning" virus would mean that individuals are always in contact with one another. As mentioned, the probability of an individual to get infected by an already infected node is the same for everyone within the population. In a network it means that an infected node can infect every other node in the network without topological restrictions, since all nodes are linked with one another either directly or indirectly.

There are three basic security mitigation practices against the random scanning worm dissemination: i) Remove, ii) Patch and iii) both Patch and Remove. Under the SIR and SIS models, a susceptible node can either be patched against the certain worm and become immune to it or stay in the susceptible state, respectively. If a susceptible node is infected then it can either stay infected and consequently spread the worm, or it can use the removal tool (e.g. an antivirus) in order to remove the worm. However, the removal tool does not encompass immunisation functionality. Thus, when an infected node removes the worm it returns back to the susceptible state, where it can subsequently be reinfected. However, if an infected node uses both the remove tool and the patch against the worm then it moves to recovery state, where it is immune against the specific worm. For each of the three security strategies differential mathematical expressions are set up, as in SIR and SIS models, which describe the dynamics of the system.

Malware Proliferation with Patch Strategy

When the Patch Strategy is used, susceptible nodes become immune to the worm, but infected nodes cannot recover from the infection. In this case, the worm and the defender seem to take part in a race. If the worm spreads very fast, it will infect most computers in a short time before defenders notice it; if people in the network can patch their computers much faster than the worm's proliferation, the wide-range infection can be avoided. The model is depicted in Figure 38.

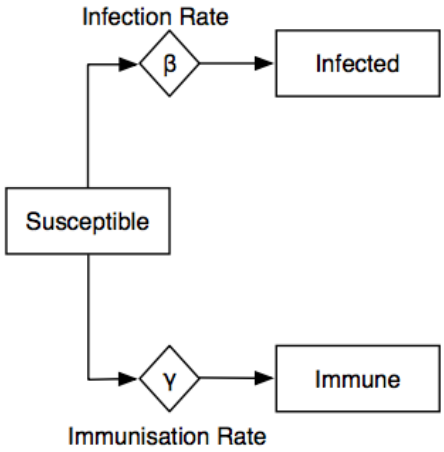


Figure 38: Patch Strategy Model

The mathematical specification of the Patch Strategy is given in Equations (34), (35) and (36), where S is the susceptible population, I is the infected population, R is the immune population. β is the probability that a susceptible node gets infected in each time unit, also regarded as infection rate, and γ the immunisation rate.

$$\frac{dS}{dt} = -\beta IS - \gamma S \tag{34}$$

$$\frac{dI}{dt} = \beta IS \tag{35}$$

$$\frac{dR}{dt} = \gamma S \tag{36}$$

Malware Proliferation with Removal Strategy

When the Removal Strategy is used, infected nodes can recover from the infection when the worm is detected and removed. However, nodes that have recovered from an infection are still susceptible to the specific worm, since no immunisation against it is included. In this case the model is transformed into a SIS model where the system reaches an equilibrium where the number of infected nodes and the number of susceptible nodes stay almost constant (Figure 39).

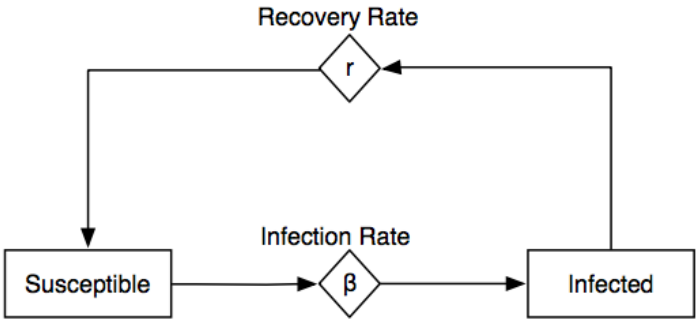


Figure 39: Removal Strategy Model

The mathematical specification of Removal Strategy is given in Equations (37) and (38). Again, *S* refers to the susceptible population, *I* refers to the infected population, β is the probability that a susceptible node gets infected every time unit and *r* is the removal or recovery rate. As seen, no recovered population is found in the system.

$$\frac{dS}{dt} = -\beta IS + rI \tag{37}$$

$$\frac{dI}{dt} = \beta IS - rI \tag{38}$$

Malware Proliferation with Patch and Removal Strategy

The last strategy devised is the Patch and Removal. In this strategy both moves of patch and removal are available. A susceptible node can become immune to the worm when the patch is used. Furthermore, an infected node can recover from the infection if the worm is removed and then become immune to the worm by using the patch. This is the most efficient, yet costly, way to eliminate malware spread. Eventually, all nodes in the network will be immune against the specific worm. The strategy model is shown in Figure 40.

The differential equations that describe the dynamics of the model are shown in Equations (39), (40), (41) and (42). *S* refers to the susceptible population, *I* refers to the infected population, *R* is used for the recovered and immunised population and Q for the

population that becomes immune to the malware. As before, β is the infection rate, γ refers to the immunisation rate when a susceptible node uses the specific patch and λ is the "removal and patch" rate.

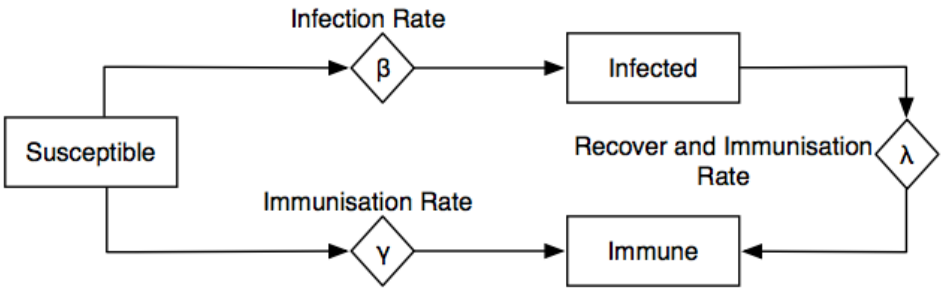


Figure 40: Patch and Removal Strategy Model

$$\frac{dS}{dt} = -\beta IS - \gamma S \tag{39}$$

$$\frac{dI}{dt} = \beta IS - \lambda I \tag{40}$$

$$\frac{dR}{dt} = \lambda I \tag{41}$$

$$\frac{dQ}{dt} = \gamma S + \lambda I \tag{42}$$

Unified Malware Proliferation Model

By combining the aforementioned mitigation strategies we constructed a unified malware proliferation probabilistic model, where each of the strategies is chosen by the defender with a probability *P*, based on the patching and immunisation rates. In this model there are three states, the susceptible compartment, the infected population and the immunised. The state transitions of the model are depicted in Figure 41. A susceptible node can either be infected with infection rate β or immunised with immunisation rate γ. An infected node can either be disinfected and immunised with rate λ or just disinfected

with rate *r*. Lastly, an immunised node cannot transit in any other state. The emerging dynamics are described by the differential Equations (43), (44) and (45).

By observing the model, it can be seen that the defender can control the disinfection and immunisation rates (γ, λ, r), while the attacker controls the infection rate (β). These rates will form the strategies of the players in the game model.

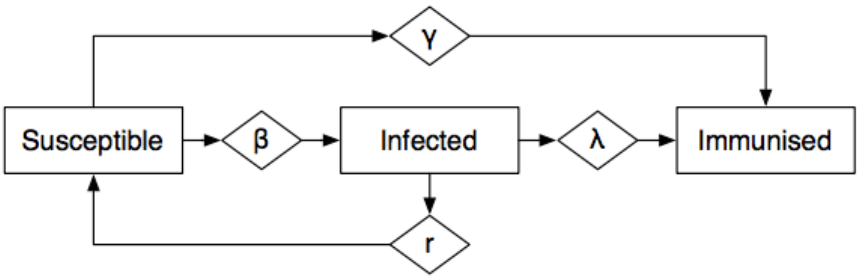


Figure 41: Unified Malware Dissemination Model

$$\frac{dS}{dt} = rI - \beta IS - \gamma S \tag{43}$$

$$\frac{dI}{dt} = \beta IS - \lambda I - rI \tag{44}$$

$$\frac{dR}{dt} = \lambda I + \gamma S \tag{45}$$

Game theory takes into account all the possible outcomes in order to find the optimal strategies. These strategies represent the NE of the game. All possible outcomes are computed and the NE is found by the pair of strategies from which, if either players deviates will always get less payoff.

Figure 42 presents the state of the system for a specific configuration for both players (the attacker has chosen $\beta = 0.00016$ and the defender $r = 0.56$, $\gamma = 0.4$, $\lambda = 0.08$). Although there is an initial increase of the infected population, the infection starts to decrease after the 16th day, mainly due to the impact of immunisation. A change even in one of the parameters of the game could result in a whole new situation. This can be seen in Figure 43 where an increase of the infection rate (β) to 0.0003 for the attacker, leads to

a significant increase of the infected population, when compared to the case where β = 0.00016. At the same time, the cost for the attacker increases, since for the increase in the infection rate an algorithm of higher complexity than before has to be utilised.

Nevertheless, in the case where β = 0.0003, if the defender increases one of his own parameters as well, that could again lead to a significantly different state of the system. For example, Figure 44 depicts the state of the system when the defender increases his immunisation rate (γ) from 0.4 (in Figure 43) to 1.2. The final state of the system is better than in Figure 43, since the final infected population is less. However, at the same time this increases the cost to the defender, since increasing the immunisation rate requires additional resources.

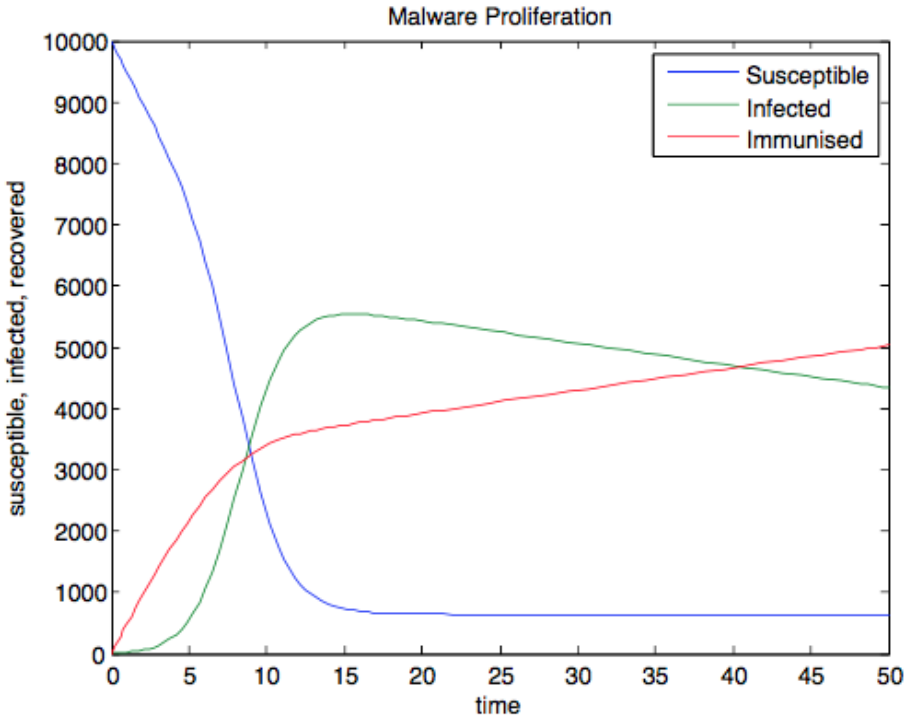


Figure 42: β = 0.00016, r = 0.56, γ = 0.4, λ = 0.08

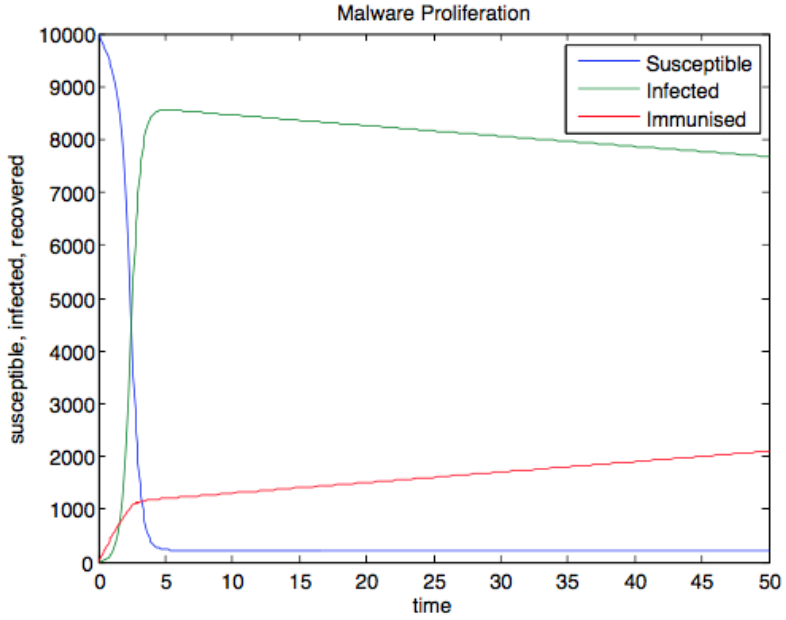


Figure 43: β = 0.0003, r = 0.56, γ = 0.4, λ = 0.08

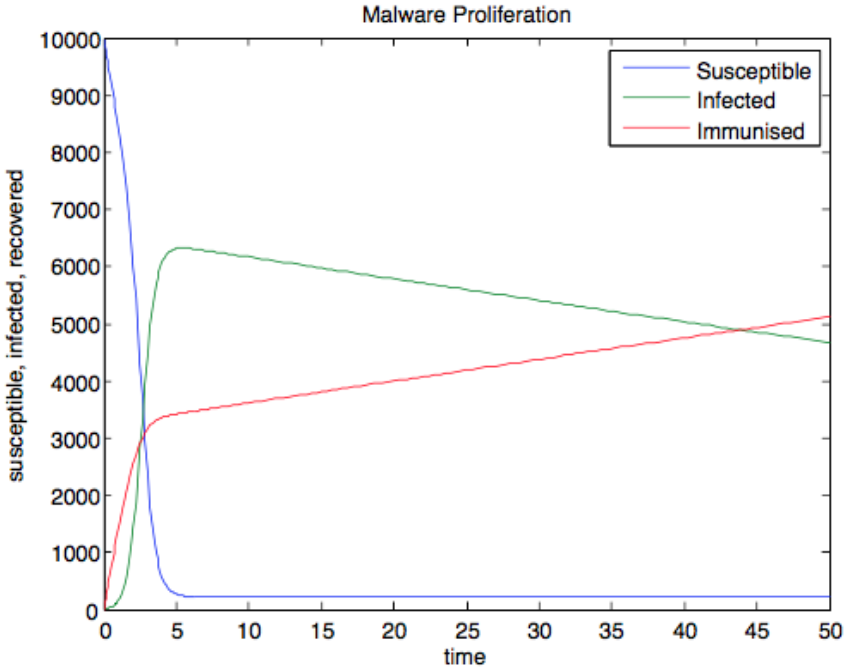


Figure 44: β = 0.0003, r = 0.56, γ = 1.2, λ = 0.08.

FLIPIT: Game-theoretical Cost Benefit Analysis

In FLIPIT [158], two opponents compete to gain full control of a shared resource and gain is defined by the time the resource is under one's control. In our epidemiology model, the shared resource is the population of nodes in the network. Each time unit, the two opponents (attacker and defender) perform actions to take under their control a part of the population. The population under the attacker's control is denoted as the infected population and corresponds to the Infected (I) compartment in the unified malware proliferation model presented above. Therefore, the gain for the attacker when spreading malware in a network is represented by the I compartment of the model. On the other hand, if N is the initial population then $N - I$ is the population under the defender's control. This population includes both the Immunised (R) and the Susceptible (S) states of the unified model. As the population in each compartment changes in time according to the dynamics described by the above equations, the total gain of each player is defined by the average fraction of node population under one's control. Therefore, by considering player 0 as defender and player 1 as attacker we define $G_i(t)$ the gain of player i and calculate it as shown in Equation (46), where $P_i(t)$ is the fraction of population under control by player i over time and t_k is the total time for which our model is running.

$$G_i(t_k) = \frac{1}{t_k} \int_0^{t_k} P_i(t)\, dt \tag{46}$$

As there are only two fractions of populations, one under the control of the defender and one under the control of the attacker, then $P_0(t) = 1 - P_1(t)$. Hence: $G_0(t) + G_1(t) = 1$.

Before the game, both players pick their strategies in order to optimise their outcome. The game is non-cooperative, static, imperfect, complete information, and not a constant-sum game. There is no cooperation between the players (network security games fall under the category of noncooperative games because there is, obviously, no cooperation between attacker and defender) [2]. As we have a static game, players have a precomputed move list (each move denoted as a strategy) from which the best move is

chosen to maximise their personal benefit. Both players choose their strategies before the game in a one-shot fashion, not being able to change them during the game. It is an imperfect game as the two players choose their strategies simultaneously, without knowing the choices of the other players. However, they are aware of the opponent's available strategies and payoffs; therefore, it is a complete information game. Finally, it is not a constant-sum game because the sum of the players' rewards is not always the same, for any combination of their strategies. In general, a pure Nash Equilibrium does not necessarily exist for this kind of games. Nevertheless, it exists in our case study.

Accounting for all actions of all possible strategy combinations (β, r, γ, λ), the optimally defensive strategy can be identified and it will be the one that returns the maximum possible gain under the minimum possible cost, regardless of attacker's chosen strategy.

Defining the Players' Strategies

In the beginning, both players choose their strategies, namely (γ, λ, r) for the defender and (β) for the attacker.

More specifically, player 0 (defender) can manipulate the immunization rate of two compartments: the susceptible population by immunizing susceptible nodes before the spread of the worm (represented by γ in our unified model) and the infected population by disinfecting and then immunizing the infected nodes (represented by λ in our unified model). Furthermore, the defender can disinfect infected nodes with disinfection rate r. Therefore, his strategy is defined by those three parameters in the unified malware proliferation model. Choosing them wisely can increase the player's benefit. However, each of these actions costs, what is known as security cost. In this work, the cost of immunisations is considered higher (a more resource demanding operation) than the cost of disinfection since it entails patching the vulnerability. In some scenarios for instance, patching an organization's mission critical host can become prohibitively costly.

On the other hand, player 1 (attacker) has the ability to manipulate the infection rate (denoted by β in our model) of the malware, by choosing among different random scanning worms with different infection rates. The infection rate of each scanning worm may depend on the vulnerability it exploits and the randomization mechanism it uses. Therefore, the higher the infection rate, the higher the software complexity of the malware

and consequently the cost of deploying the attack increases. For that reason, the attacker aims to find the infection rate that will return the optimal payoff.

Defining the Players' Payoffs

As mentioned, both players' strategies bear some cost. We define cost $C_0(t)$ as the total number of moves made by player 0 as $C_0(t) = n_{0,1}(t) + n_{0,2}(t) + n_{0,3}(t)$ where $n_{0,1}(t), n_{0,2}(t)$ and $n_{0,3}(t)$ correspond to the number of disinfections, immunizations, and disinfections and immunizations, respectively, multiplied by each move's cost $(k_{0,j})$ (Equation (47)). The move's cost is defined as the cost of disinfecting $(k_{0,1})$, immunizing $(k_{0,2})$, or disinfecting and immunizing $(k_{0,3})$ a node.

$$C_0(t) = n_{0,1}(t) \cdot k_{0,1} + n_{0,2}(t) \cdot k_{0,2} + n_{0,3}(t) \cdot k_{0,3} \quad (47)$$

We define as cost for player 1 the perceived complexity of the algorithm that the malware implements. The complexity of the algorithm is commensurate with the infection capabilities of the malware. Therefore, the higher the infection rate of the worm is, the higher is also the cost, k_1, that attacker has to pay in order to implement the malware (Equation (48)).

$$C_1(t) = k_1 \quad (48)$$

Each player's payoff is equal to the player's total gain minus the related cost according to Equation (49).

$$B_i(t) = G_i(t) - C_i(t) \quad (49)$$

To compute costs, we use quantitative tables of operational complexity. A strategy by either player (e.g., Patch Strategy for the defender or Code-Red worm for the attacker) may encompass several actions, with each action characterised by a complexity level. For practical reasons, we set up empirically three levels of perceived complexity (low,

medium, and high) and assign a score to each of 1, 2, or 3, respectively. Therefore, the cost of a move for player 0 or the total cost of player 1 is equal to the sum of the costs of the actions it involves. An example is given in Table 11 and Table 12, where we present the actions cost for the defender and the attacker when the latter uses the Code-Red worm (in which case the attacker has already chosen her strategy).

Table 11: The cost for Code-Red worm

Actions	Complexity			Total
	Low:1	Medium:2	High:3	
Exploit the buffer vulnerability		2		
Generate random IP addresses	1			4
Launch 99 threads with IP addresses	1			

Table 12: The cost of each move for the defender

Actions		Complexity			Total
		Low:1	Medium:2	High:3	
Patch	Detection		2		4
	Patch		2		
Removal	Detection		2		3
	Reboot	1			
Patch and Removal	Detection		2		5
	Reboot	1			
	Patch		2		

As in FLIPIT, the gain is defined by fraction of population under each player's control. The population under the attacker's control corresponds to the infected population, while the population under the defender's control corresponds to the susceptible plus the immunised population.

In order to find the defender's strategy that will return the optimal payoff, known as the Nash Equilibrium strategy, we construct the description of the game, which is a table with all possible payoffs for both players for all the available combinations of strategies. More details on how these strategies are calculated, can be found in the following section.

Case Study

In this section we apply our game-theoretical malware proliferation model to a real case scenario, where the attacker can choose between five hypothetical worms with different infection rates (β). For the determination of the infection rates we used as a reference the Code-Red worm. According to [162], a node infected by this worm infects other nodes with rate 1.62 nodes per hour. Albeit old, we have chosen Code-Red because it is a random-scanning worm with no topology constraints and, thus, its characteristics fit well into the generic nature of our abstraction. Its behaviour has also been thoroughly studied in the past [162][163][164].

In the examined scenario, the defender (e.g. the ICS vendor), tries to prevent the spread of the malware within the corporate network (S_4) in which 10,000 nodes are deployed, taking the corresponding security costs into account. Therefore, the probability that a susceptible node in the network gets infected by an infected one, in each second, is $1.62/N$, where N is the total population. Thus, $\beta = 1.62/N = 1.62 \cdot 10^{-4}$.

To provide the attacker with more options, we make the assumption that she can choose among five different types of worms, whose propagation rates are equal to integral multiples of Code-Red's propagation rate. As a result, the attacker can choose from five different worms and her available strategies are described as $\beta = k \cdot 1.62 \cdot 10^{-4}$, where $k = 1,2,3,4,5$.

Moreover, we assume that the defender can determine his strategy by choosing the immunization rate ($0 \leq \gamma \leq 100$ immunisations/hour), the disinfection rate ($0 \leq r \leq 100$ disinfections/hour) or/and the combination of both disinfection and immunisation with rate $0 \leq \lambda \leq 100$ per hour. In reality these rates can potentially get higher values, depending on the capabilities of the stakeholder. However, for the purposes of our experiment we limit all three rates from 0 to 100.

To simplify the scenario, we predetermined that the cost for the attacker is equal to $\beta \cdot 1000$, implying that the propagation rate of the attack affects the complexity of the algorithm that implements the attack. We also make the assumption that the cost of a disinfection is 10 and the cost of an immunisation is 100 (considering that immunisation costs more than disinfection). Table 13 forms the description of the game. Each cell within the table corresponds to a pair of payoffs, one for the attacker and one for the

defender, for the specific pair of strategies. For instance, $P_{A_{1,1}}$ corresponds to the attacker's payoff when the attacker chooses the strategy $\beta = 1.62$ and the defender chooses the strategy ($\gamma = 0$, $r = 0$, $\lambda = 0$). The defender's payoff for the same pair of strategies is $P_{D_{1,1}}$.

Table 13: The description of the game

		Defender (γ,r,λ)				
		(0,0,0)	(1,0,0)	(2,0,0)	...	(100,100,100)
Attacker (β)	1.62	$P_{A_{1,1}},P_{D_{1,1}}$	$P_{A_{1,2}},P_{D_{1,2}}$	$P_{A_{1,3}},P_{D_{1,3}}$	...	$P_{A_{1,10^6}},P_{D_{1,10^6}}$
	3.24	$P_{A_{2,1}},P_{D_{2,1}}$	$P_{A_{2,2}},P_{D_{2,2}}$	$P_{A_{2,3}},P_{D_{2,3}}$	...	$P_{A_{2,10^6}},P_{D_{2,10^6}}$
	4.86	$P_{A_{3,1}},P_{D_{3,1}}$	$P_{A_{3,2}},P_{D_{3,2}}$	$P_{A_{3,3}},P_{D_{3,3}}$	...	$P_{A_{3,10^6}},P_{D_{3,10^6}}$
	6.48	$P_{A_{4,1}},P_{D_{4,1}}$	$P_{A_{4,2}},P_{D_{4,2}}$	$P_{A_{4,3}},P_{D_{4,3}}$	...	$P_{A_{4,10^6}},P_{D_{4,10^6}}$
	8.1	$P_{A_{5,1}},P_{D_{5,1}}$	$P_{A_{5,2}},P_{D_{5,2}}$	$P_{A_{5,3}},P_{D_{5,3}}$	...	$P_{A_{5,10^6}},P_{D_{5,10^6}}$

It is worth noting that a different selection of the parameters of this case study would obviously change the outcome of the game, without however changing the principles of the proposed model. These parameters are given here not as a reference, which falls outside the scope of this work, but to demonstrate the application of our unified model against malware proliferation. The parameters depend on each malware proliferation scenario, namely depend on the skills and goals of the attacker and the risk status of the defender (organization, individual).

For the simulation of the epidemiology model we used the Ventana Simulation Environment (Vensim). The simulations are based on Equations (43), (44) and (45), with total population of 10,000 nodes, 5 of which were initially infected. For the possible values of β, γ, r and λ we run the model for $t_k = 168$ *hours* $= 7$ *days*. Vensim produces the data that are needed to set up the game. More particularly, it provides the infected, disinfected and immunised populations per unit time (in our case the software is set to run the simulations per hour). Therefore, the total number of disinfections ($n_{0,1}(t_k)$), immunisations ($n_{0,2}(t_k)$) and 'immunisations and disinfections' ($n_{0,3}(t_k)$) in those 7 days can be found. Vensim also returns the infected ($P_1(t)$) and uninfected ($P_0(t)$, susceptible plus immunised) populations per unit time.

Based on the results from Vensim, the related costs and gains for both players can now be computed. For every combination of strategies (β, γ, r and λ), Vensim returns the $P_1(t)$ and $P_0(t)$ values, which are used to calculate the gain for each player according to

Equation (46). As mentioned, it also returns the values $n_{0,1}(t_k)$, $n_{0,2}(t_k)$ and $n_{0,3}(t_k)$, which, in conjunction with the assumed cost of disinfection ($k_{0,1} = 10$) and cost of immunisation ($k_{0,2} = 100$ and therefore $k_{0,3} = 110$) and based on Equation (47), return the defender's cost. Based on Equation (48) and our assumptions about the attacker, the attacker's cost for the different values of β is equal to $\beta \cdot 1000$. The gain of each player, as mentioned earlier, is equal to the mean fraction of population under each player's control. Thus, for every different combination of strategies we can now compute the related payoffs for both players according to Equation (49), populating the Table 13.

In order to solve the game, the Lemke-Howson algorithm was used, which returns Nash Equilibria for two-player non-zero-sum games [165][166] [167]. The algorithm (implemented in MATLAB) takes Table 13 as input and returns the Nash Equilibria of the game.

The results revealed a unique pure NE that corresponds to the optimal strategy for the defender, represented by the values $\gamma = 10$ immunisations/hour, $r = 100$ disinfections/hour and $\lambda = 10$ "disinfections followed by immunisations"/hour with *payoff* $= -5.44 \cdot 10^3$. Our experiment suggests that even though the proactive immunisation should be preferred to the other two actions for security reasons, it does not get the maximum value. In fact, the game results in a NE where the disinfection rate (r) is larger than the immunisation rates, meaning that security costs have changed the optimal solution for the defender. On the other hand, the attacker's optimal strategy is to choose $\beta = 8.1$ which is the maximum infection rate in the table. This happens due to the fact that in this particular experiment, the attacker's gain is much higher than the cost of her strategy and, therefore, she will always get larger payoff by choosing the worm with the highest infection rate. If the cost of attack is much higher (for instance in case the attacker can choose a zero-day attack), the resulted NE may differ.

3.3.3.3 Findings and Conclusions

In this work, malware proliferation models have been integrated with game theory in order for a cost-benefit approach to be developed. With this approach we managed to evaluate defense strategies that mitigate malware proliferation in the corporate network. We demonstrate the application of our approach with a case study focusing on minimising

the effect of random scanning worms (such as Code-Red worm) infecting a corporate network of 10,000 susceptible hosts. In this scenario, both the defender and the attacker can choose among a variety of strategies in order to achieve their individual goals. The results of the case study highlight that the cost of security restricts the security level of the defender, since the resulted optimal strategy does not correspond to the most secure one; it is however the one that offers the highest possible security under the least possible cost, regardless of the attacker's strategy.

An interesting extension of this work could be the introduction of a security level threshold in the game eliminating the strategies that correspond to gains that do not meet the defender's requirements. In addition, applying the model against other worms and other strategies is expected to produce different, but still interesting results, but this falls outside the scope of this work.

Another idea could be to incorporate topology-oriented malware that spreads more efficiently within networks. The logic would still be the same; a topology-oriented malware dissemination model will feed our game with the necessary parameters. This game would then, again, return the optimal defense strategies. In any case, Game Theory under traditional malware proliferation approaches can make those models an extremely useful tool for the efficient and effective protection of networks.

3.4 Conclusion

All in all, in this chapter, our security-oriented contribution is presented through the corresponding use cases. These use cases include models that apply on WSNs (approaches using Game Theory on IDS and IPS) and CI-ICSs (approaches using the combination of VSM and Game Theory, Monte Carlo predictive modelling and also the combination of Epidemiology and Game Theory). As a result, the identified gaps of the existing approaches have been mitigated and RQ2 has been answered.

4 Chapter

SYSTEMS RESILIENCE AND OPTIMIZATION

Chapter 4 includes the proposed models on improving systems from a non-security perspective. It examines this topic within the context of improving the resilience of WSNs (specifically, energy efficiency, packet loss and processing time) and a novel application on using Hot-Desking in order to increase employees' productivity in a work environment. Within this chapter, RQ3 is addressed.

This chapter includes material from the following published papers, as per below:

Section	Published Paper
4.2	Haghighi, M., Maraslis, K., Tryfonas, T., & Oikonomou, G. (2015). Game-theoretic approach towards energy-efficient task distribution in wireless sensor networks. In 2015 IEEE SENSORS (pp. 1–4).
4.2	Haghighi, M., Maraslis, K., Tryfonas, T., Oikonomou, G., Burrows, A., Woznowski, P., & Piechocki, R. (2015). Game-theoretic approach towards Optimal Multi-tasking and Data-distribution in IoT. In 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT) (pp. 406–411). IEEE..
4.3	Maraslis, K., Cooper, P., Tryfonas, T., & Oikonomou, G. (2016). An Intelligent Hot-Desking Model Based on Occupancy Sensor Data and Its Potential for Social Impact. In Transactions on Large-Scale Data-and Knowledge-Centered Systems XXVII (pp. 142–158). Springer
4.3	Cooper, P. B., Maraslis, K., Tryfonas, T., & Oikonomou, G. (2017). An intelligent hot-desking model harnessing the power of occupancy sensing data. Facilities, 35(13/14), 766–786.
4.2	Maraslis, K., Haghighi, M., Tryfonas, T., & Oikonomou, G. Game-theoretic and Auction-based Algorithms towards Autonomous Decision-making in WSNs. (To be submitted)

4. Systems Resilience and Optimisation

The previous chapter was about the security and risk management perspective of a system. This one will be about their resilience and optimisation perspective, instead. Firstly, there is a focus on the resilience and optimisation of WSNs and later there is a section on Hot-Desking.

4.1 Introduction

In the bibliography, there is a wide variety of methods that are used in order to improve different aspects of a system. In this chapter, we present some custom methods, using which we bring an improvement on energy consumption, agent processing time and packet loss within a WSN with only a minor (in most cases) increase in latency, as well as a fresh and innovative look at the concept of Hot-Desking which brings significant improvement on the employees' productivity, as defined in the work itself.

4.2 Wireless Sensor Networks

In this section, there is firstly an introduction on WSNs and after that the presentation of the modelling methods using SensomaX along with their evaluation after being applied on specific scenarios.

4.2.1 Introduction

WSNs have become a major technology for a wide variety of applications, ranging from medical to military and environmental monitoring. Conventional applications often involved a limited number of sensors spread across an area of interest, in order to gather various parameters in a central unit and they mostly performed simple functionalities such as calculating the average variation of a parameter from different sensors.

Modern applications however, require data to be aggregated online, and often require a number of actions to be applied on the environment (i.e. via actuators) as a result

of the data aggregation process. Therefore, they should be able to handle much more sophisticated set of logical and mathematical functionalities, often implemented in a collaborative fashion, amongst a large number of sensors and actuators. Such functionalities necessitate a relatively powerful processor and sufficient memory for retrieving raw data and storing the processed ones. As such, sensor nodes need to be equipped with more capable components compared to conventional WSNs. In addition to the need for extra components, such advanced functionalities are power-hungry processes, which consume considerable energy in order to handle the high footprints on the memory and processor.

In this section we use auction-based techniques [168][169] with Game Theory to optimise multi-tasking, distribute applications' tasks amongst sensors based on their available resources, investigate how quickly and energy-efficient applications' requirements can be served and improve energy efficiency.

4.2.2 Proposed Model

The content of this section addresses part of RQ3 by demonstrating how utilising auction-based techniques along with SensomaX, can improve energy consumption, agent processing time and packet loss in WSNs with an increase in latency that is considered trivial in most cases.

Before we go deep into any low-level details, it is worth mentioning that serving the end-users is considered the most important requirement of the base station. Therefore, the base station needs to satisfy the services required by the end-user as its first priority. However, new applications, which are deployed onto the base station, either by the existing end-users or the new ones, have certain requirements that also need to be satisfied in addition to the pre-deployed applications.

In the context of game theory, the base station should weight its strategies and choose the best option, which maximises or at least maintains its profit (utility) whilst meeting old and new applications' requirements simultaneously. A node's utility is

defined by the amount of processing time spent on the given tasks, where maximising utility means spending less processing time, thus saving more energy.

As was briefly pointed out, the decision (strategy taken) of the base station will be known to the Cluster-Heads. The same applies to the communications between the Cluster-Heads and their members. Therefore, in this section we will consider maintaining or maximising the base station, Cluster-Heads' and cluster members' utilities in an extended game-theoretic form with perfect information.

As explained earlier, our proposed approach uses auction-based algorithm in conjunction with Game Theory. The auction-based algorithms are only used to calculate the price of each task. When the base station receives an application from the end-user, it initially needs to query all the Cluster-Heads with the operational details of the new task, in order to collect their offers for the task. Cluster-Heads advertise their offers based on their on-going operations and the number of applications running concurrently. Once all offers are collected, the base station starts the task distribution process by initially applying the game-theoretic approaches in order to identify its options, or in other words, its strategies, as defined by the game theory.

Every application is comprised of a number of tasks, which can be priced based on its given operational paradigms. Therefore, each task has a certain value regardless of every node's operational state. Once applications arrive in the base station, their tasks are priced, and offers are collected from the Cluster-Heads.

For this case study, full details of the game will be given in order to establish a better understanding of how interaction works amongst the sensor nodes. Also, the game is implemented in a simplified form with low network density.

All nodes are initially assumed to be indifferent in terms of their capabilities, their on-going operations, number of concurrent applications and their remaining energy level. Hence, for the first phase of this experiment we will demonstrate the interaction between the base station and a single Cluster-Head in order to identify their available strategies with perfect information. This interaction can be envisioned as a game between the base station and the Cluster-Head, where both network entities' rewards calculated based on the task price and the available resources in the node. In the second phase, the game will expand to include more nodes, thus creating a wider interaction amongst network entities.

The Cluster-Head used in this experiment is already running an application, which requires registering Temperature at 5-second intervals, and forwarding the recorded data to the base station at 60-second intervals. This application is hereafter referred to as the 'pre-deployed' application. Assuming that the base station receives a new application, which requires recording Light level, with the same timing and recording requirements as the previously deployed application, here we will analyse the interaction of the base station and the Cluster-Head in handling the new application.

The maximum utility (reward) of every Cluster-Head is achieved by minimising the processing time, thus saving more energy for longer lifetime, whereas the maximum utility of the base station is directly related to serving the end-users' application requirements.

The decision-makings done by the network entities (including the base station, Cluster-Heads and the nodes) for handling the new task, will narrow their choices down into prioritising their given tasks.

The base station can make its selection from the following strategies:

A. Receive the task and never relay it to any CH (Priority 0)
B. Accept the task and relay it immediately (Priority 1)
C. Accept the task and delay its relay with minor latency (Priority 2)
D. Accept the task and delay its relay with major latency (Priority 3)

The priority number appearing next to each option indicates the execution priorities based on SensomaX's internal architecture. Priorities define how urgently the tasks need to be executed, and effectively assign their position in the execution queue. Similarly, the Cluster-Head also has the above-mentioned options as the base station, except that, instead of relaying the given tasks to another node, it executes them internally, which results into the following strategies:

a. Receive the task and never execute it (Priority 0)
b. Accept and execute the task immediately (Priority 1)
c. Accept the task and delay its execution with minor latency (Priority 2)

d. Accept the task and delay its execution with major latency (Priority 3)

Given the above strategies for both the base station and the Cluster-Head, and assuming that the entities cannot reverse their decisions (static game), and the new application has a lower priority to the pre-deployed one, the interaction can be demonstrated as shown in Figure 45. Rewards are shown in parentheses with the first figure denoting the base station's reward - BSR - and the second standing for the Cluster-Head's reward - CHR - in the form of: (BSR, CHR).

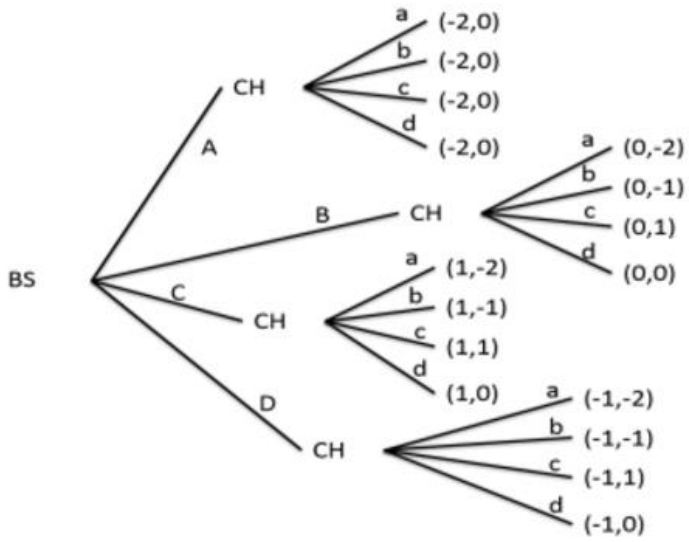


Figure 45: Base station and Cluster-Head in a game-tree

As this figure depicts, the base station's maximum reward leans towards taking strategy 'C' with payoff 1, whereas the Cluster-Head's maximum rewards can be achieved by taking strategy 'c'. That is because, if the base station takes strategy 'C', it in fact serves the end-user's requirements to the best of its capability and maintains serving the pre-deployed application as well, compared to relaying the task with no or major delays, or not relaying the task at all. The same applies to the Cluster-Head, whereby taking strategy 'c', which executes the application with minor delay, allows it to first execute the pre-deployed task and then act on the new one. Whereas taking other strategies either delay the current task (b), never executes the new task (a), or executes the new task with a major delay (d). In case 'a', although not executing the task results in less energy consumption, the Cluster-Head is still acting against the base station

requirements and will result in being queried frequently for the given task's progress (which results in spending energy on processing the queries), and it could be assumed faulty by the base station and ultimately excluded from the network. Given the above explanation, there is a single dominant strategy, which is also the Nash equilibrium: (C, c) resulting in maximum payoff for both network entities. This is because both entities cannot maximise their payoffs by unilaterally changing to other strategies other than taking the (C, c) strategy. This equilibrium is achieved in an extensive form of the game-theoretic approach with perfect information.

Figure 45 demonstrates the rewards of network entities in simple numerical values as a result of the hierarchical decision-making between the base station and Cluster-Head. The actual pricing scheme however, differs immensely, which results in greater quantities of payoffs.

Applying the auction-based pricing equations [168][169] to the aforementioned application, results in the following figures for the base station and the Cluster-Head:

Table 14: Processing times

	Base Station	Cluster-head
Available Processing Time (P_a)	5000	1000
Pre-deployed Task's Required Processing Time (P_d)	2500	500
New Task's Processing Time (P_t)	2500	500
Query/Response Processing Time (P_q)	500	100
Total Energy (E_{total})	N/A	100,000

It is worth noting that the actual processing time in SensomaX's architecture has been defined in milliseconds. However, for simplicity the above figures are normalised by a factor of 1,000,000.

Once nodes' utilities and tasks' prices have been calculated using the aforementioned auction-based techniques, the rewards gained by the peers, based on the notations given in Table 14, can be calculated using the following function:

$$E_{saving} = P_a - \left[\left(\frac{\sum_{i=0}^{i=n} P_{d_i}}{n} + \frac{\sum_{j=0}^{j=m} P_{t_j}}{m}\right) + \sum_{k=0}^{k=s} P_{q_k}\right] \quad (50)$$

This function simply returns how much energy can be saved by taking into account the number of pre-deployed tasks (n), new tasks (m) and the total number of query/responses (k). Having calculated the total saved energy, node's remaining energy can be calculated by deducting the saved energy from the total energy:

$$E_{Remaining} = E_{total} - E_{saving} \quad (51)$$

For the purpose of this model, we will not deal with the remaining energy, and the only focus will be on the saved energy, which is considered as the reward. Based on the actual pricing units, which were shown in Table 14, the base station will compare its available strategies, whilst calculating the following rewards using the function for E_{saving}. The calculated rewards are therefore shown in Table 15.

Table 15: Actual rewards for the base station and Cluster-Head's strategies

BS / CH	A	B	C	D
a	-1000 0	0 -700	1250 -700	-500 -700
b	-1000 0	0 -500	1250 -500	-500 -500
c	-1000 0	0 750	1250 750	-500 750
d	-1000 0	0 0	1250 0	-500 0

Table 15 represents the actual rewards (profit and loss) of the base station and the Cluster-Head in normalised milliseconds and is actually the application of Table 14 on equation 50. In this table, we can again see that, strategy 'C' for the base station and strategy 'c' for the Cluster-Head result in maximum rewards.

What has been described so far only included the interaction between the base station and a single Cluster-Head. In order to expand the game to involve more players, the base station iterates the same process for every Cluster-Head involved in the task distribution process.

Case Studies and Evaluation

In this section, the investigation of the impact of latency and cluster density on different operational paradigms with and without game-theoretic utilisation will be presented, as well as the energy profiling and packet loss of nodes and Cluster-Heads using Game Theory. Firstly, we examine how effectively Game Theory can contribute towards energy consumption between the base station and Cluster-Heads. This was mainly done to optimise task distribution as the first step in which Cluster-Heads receive their tasks. As we mentioned in the previous section, task allocation can be challenging, depending on Cluster-Heads' properties, such as their remaining energy and pre-deployed tasks. Therefore, we have built two separate applications. The first one is deployed and executed as the pre-deployed application, and the second application is deployed whilst the first one is still running. This approach creates a situation, where nodes tend to compete, in order to take the new application's tasks depending on their available resources as the result of executing the first application's tasks.

The first application is a time-driven application, which demands light level sensory data every second upon base station's query (request), as well as requiring the sensor node to report temperature every 10 seconds without any request from the base station. The second application demands light level every 5 seconds upon base station's request, as well as requesting automatic reporting of acceleration on three-axis (X,Y,Z) every 500 milliseconds. Cluster-Heads receiving these applications query their members for the required parameters at the specified intervals. This experiment is repeated twice, with and without the game-theoretic approach involved in the execution process.

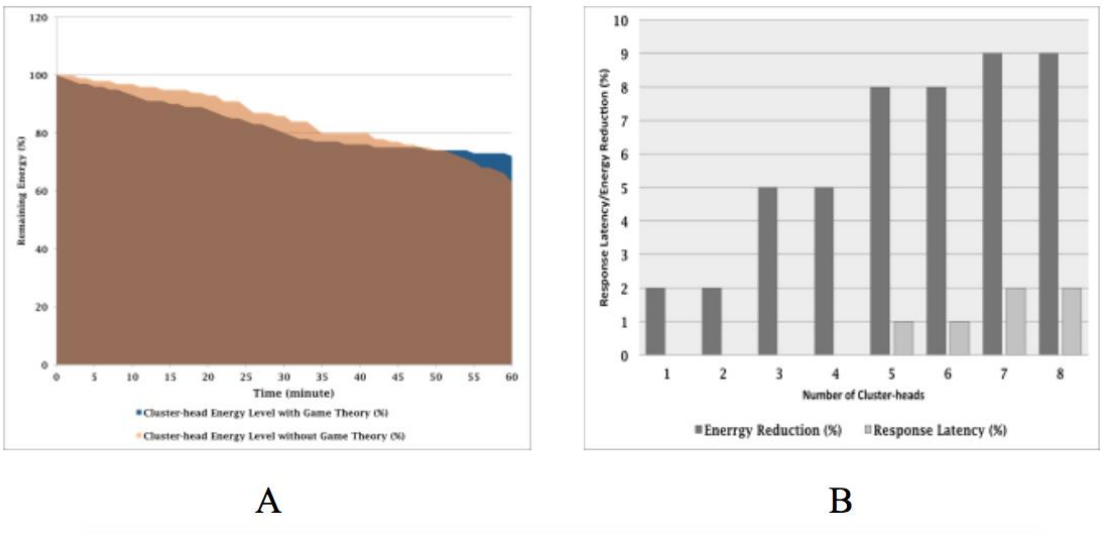
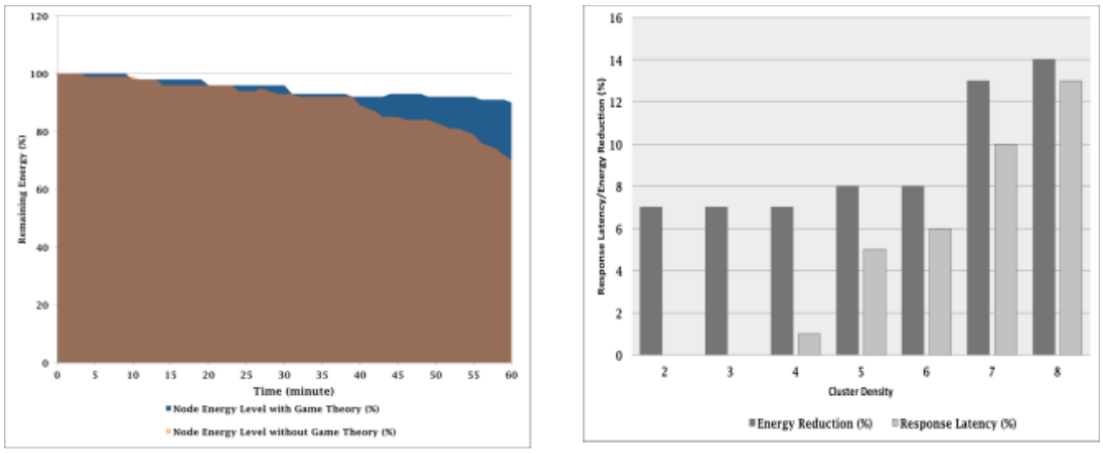


Figure 46: (A) Sensor nodes' energy profiling, (B) Energy reduction and latency associated with the number of Cluster-Heads using game-theoretic approach

Based on the explanation given in the previous section and how Cluster-Heads decide on allocating different priorities to their given tasks, the results achieved from the experiment are shown in Figure 46(A).

As a result of such trial and error iterations, and mainly due to the high number of price calculations, the energy level drops significantly in the beginning of the process. However, once a winning strategy is chosen, energy-hungry price calculating process is reduced considerably, and the Cluster-Head tends to stay with a single strategy. Therefore, as brown histogram shows, Cluster-Head's energy spending stabilises after approximately 30 minutes. In fact, the Cluster-Head achieves a better energy profiling when Game Theory is applied (blue part of the graph) compared to the non-game-theoretic approach. Figure 46(B) demonstrates the reduction in the energy consumption and the mostly insignificant increase in latency of 1-8 Cluster-Heads with and without the game-theoretic approach in a WSN. The applications used in this experiment are the same applications used in the previous experiment (Figure 46A), which were deployed in the same fashion. As Figure 46(B) shows, the dark grey bars denote the total reduction in the energy consumption of the network compared to the non-theoretic approach, whereas the light grey bar represent the latency caused in the Cluster-Heads response to the base station during the lifetime of the applications. As dark grey bars show in this figure, the higher number of Cluster-Heads (players), the higher the energy reduction becomes. That

is mainly due to the higher number of Cluster-Heads fulfilling the application, whereby game theory can facilitate task distribution amongst higher number of Cluster-Heads.



A B

Figure 47: (A) Cluster-Head energy profiling with and without game theory, (B) Energy reduction and latency associated with different cluster densities using the game-theoretic approach

The presence of more players helps the base station to locate Cluster-Heads faster. Mainly because they are already engaged in other tasks. Whereas in the non-game-theoretic mechanism, tasks are simply split up amongst Cluster-Heads with no consideration on the overhead imposed on them whilst executing other tasks.

This outcome prompts the end-users to adopt more Cluster-Heads in order to reduce the energy consumption. However, as we mentioned earlier, as the number of players increases, the timely responses of the Cluster-Heads are reduced. As the first three light grey bars on the far left side of the chart show, the response delay for 1-4 Cluster-Heads is around 1%, which can be considered insignificant. That trivial impact is with regards to the second application, where three acceleration variables (X, Y, Z) are reported every 500ms, which could sum up to 15ms. However, as the number of Cluster-Heads increase, the latency could increase to up to 2%, which can sometimes be considered quite vital, over the lifetime of the application, especially if they are considered critical.

In this experiment, each Cluster-Head was allocated two members only. The other factor we tried to focus on was how cluster density affects both energy consumption and

response latency within each cluster. Therefore, we repeated a version of the previous experiment, this time with a variable number of nodes in each cluster.

As Figure 47(B) depicts, the dark grey bars represent the total game-theoretic energy reduction with a variable number of nodes in a single cluster compared to the non-theoretic approach. According to this figure, as with the higher number of Cluster-Heads, the higher number of nodes in a cluster reduces the energy consumption significantly. The total reduction energy consumption reaches up to 14% with 8 members in a cluster, which is more than a third higher the quantity of energy saved over 8 Cluster-Heads. However, the response latency is also considerably higher. Based on Figure 46(B) and Figure 47(B), the optimal number of Cluster-Heads and cluster densities used in a WSN needs to be in the range of 1-4 Cluster-Heads, each containing 2-3 members, in order to achieve minimum latencies towards meeting application requirements.

Figure 46(A) depicts the average energy profiling of one of the three clusters in a WSN, each of which has a CH and 3 nodes reporting to it. As seen by the brown histogram, the game-theoretic approach can save nearly 15% on the energy consumption with our experimental optimal values.

The experiments reported in this section were mainly conducted using time-driven applications. The next experiment will investigate how game-theoretic approach affects energy consumptions of applications with different operational paradigms as in Table 16.

Table 16: Applications with different operational paradigms

Application	Operational Paradigm	Frequency/ Threshold	Parameter
A	Query-driven	250ms	Light and Temperature
B	Data-driven	>300ms	Light and temperature over 5 minutes
C	Event-driven	>500 <20	Light
D	Time-driven	5 seconds	Light and Temperature

The previous experiment was repeated four times, each time deploying one of the above-mentioned applications. Figure 48 shows the energy profiling of different

applications with different operational paradigms, with (black bars) and without (green bars) the game-theoretic approach.

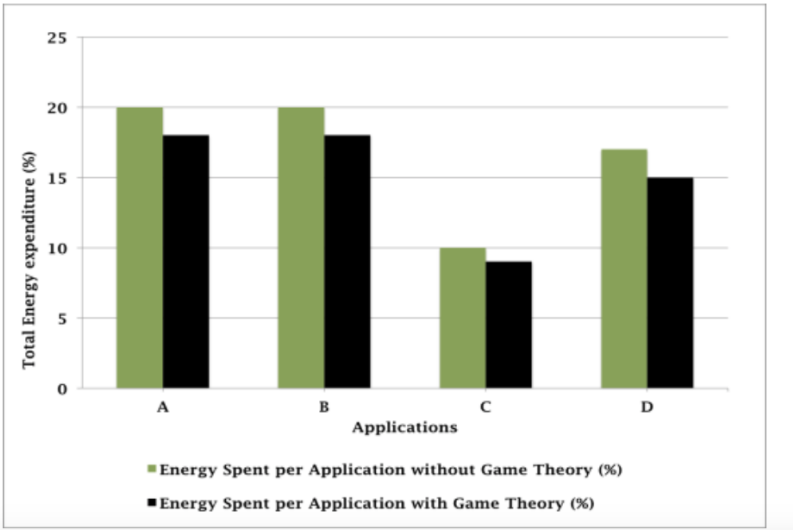


Figure 48: Energy expenditure for different operational paradigms

According to Figure 48, apart from application C, which is an event-driven application, game-theoretic approach saves around 2% on the total energy consumption of all operational paradigms. That could be because, event-driven applications involve various unexpected events, which are triggered according to the given environment. Therefore, it leaves less flexibility to the Cluster-Heads' game-theoretic mechanism in order to stabilise and adapt to the application's behaviour.

Additionally, there also exists a high number of packet collisions, which results in many data packets being lost in transition. Packet loss happens due to high number of interactions in the network, where multiple nodes communicate simultaneously.

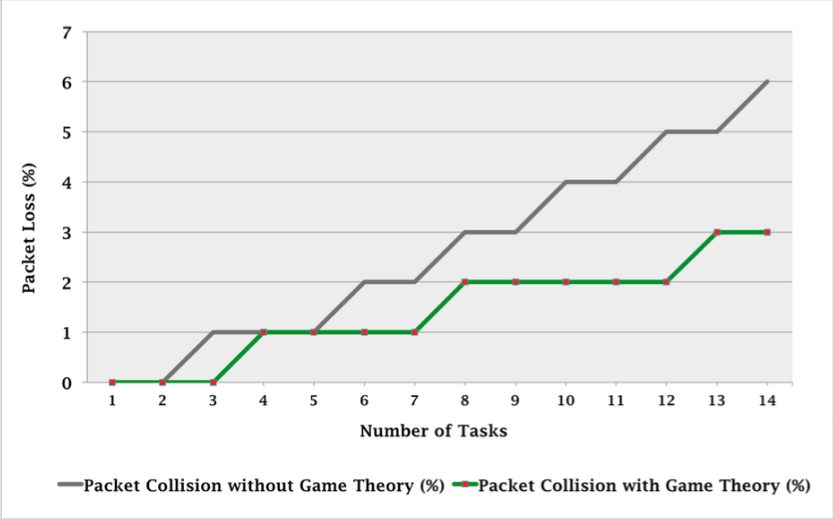


Figure 49: 'Packet'collision'with'and'without'game'theory'

SensomaX in general suffers from slight packet loss in its communication mechanism. However, since our game-theoretic approach also involves a very large number of negotiations amongst various network peers, we decided to investigate the packet loss with regards to the number of applications deployed on to the network. Figure 49 shows the amount of packet loss with (green vector) and without (grey vector) the game-theoretic approach. Based on our analysis, the game-theoretic approach slightly improves packet loss as the number of tasks is increased. In order to decrease inefficiencies in our experiment, the tasks used in this experiment were all of the same type of time-driven task. Using game theory improved packet loss by nearly 3% with 14 tasks deployed onto the network. The decrement in packet loss is primarily due to the latency, which indirectly delays the communication amongst the peers, which results in lower packet loss.

Finally, it is briefly described how auction-based algorithms could improve the processing time of each agent. Since most of the operations in SensomaX are primarily based on agents, packets transmitted around the network are all in the form of agents. Therefore, processing time of each agent according to the size of the network has a major impact on the execution of each application. Figure 50 demonstrates the average processing time of agents in simulation.

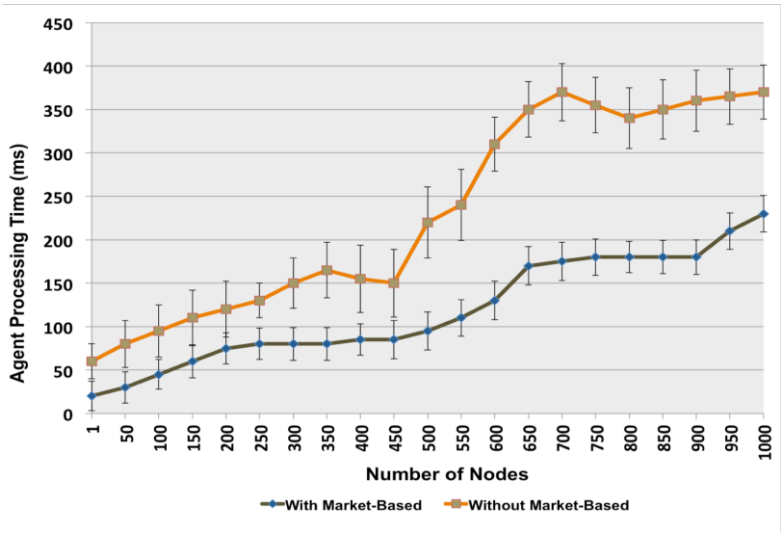


Figure 50: Agent processing time vs network size

Orange plot represents the agent processing time without market-based algorithms, whereas blue plot represents the agent processing time with market-based algorithms. According to this figure, auction-based (or market-based, it is the same in this context) algorithms improve the agent processing time significantly across the network. That is mainly due to the aforementioned smart mechanism for allocating the tasks to the cluster-members.

Findings and Conclusions

In this work we have demonstrated how utilising auction-based techniques along with SensomaX, can improve energy consumption with only a small impact on latency within a WSN. SensomaX, as a multitasking WSN middleware, can identify the optimal strategies in an autonomous decision-making process. The proposed approach exhibited how SensomaX in conjunction with Game Theory can optimally allocate resources to the deployed applications, based on nodes' processing and memory availability, as well as their remaining energy level. On top of that, we were also able to show how the model can improve agent processing time and packet loss in large scale scenarios. Further work could include applying similar techniques on WSNs with specific topologies or many different densities in order to put its applicability and scalability to the test.

4.3 Hot-Desking

4.3.1 Introduction to Hot-Desking

Due to the increasingly digital world we live in, we tend to derive value and knowledge from as many sources of data as possible. Apart from any sociological parameters, there are two key factors that enabled that trend.

Firstly, it is the Internet of Things (IoT) or in other words the idea of providing internet connectivity, not only to established IT devices such as phones and computers but also to more 'traditional', seemingly non-IT devices such as air conditioners, fridges, chairs, locks etc. [170].

Secondly, it is the rise of the so-called Big Data (BD). The constantly increasing amount of connected devices is generating an exponentially growing amount of data. This, in conjunction with the more and more sophisticated methods of analysing data and extracting knowledge, is bound to change the way we live.

Nowadays, numerous industries collect and analyse data for multiple purposes. From organisations with environmental mindfulness that try to measure and mitigate the impact of modern life-style on environment to businesses that are after the most effective methods to reduce costs and increase profits. For reference, almost 80% of the developed countries' population live in cities with the percentage falling to almost 51% in developing countries. The forecast for 2050 is 88% and 67%, respectively. In addition, the global CO_2 emissions (in metric tons) is expected to demonstrate a 46% increase from 2010 to 2030. Therefore, it is unlikely this focus is going to drift any time soon [171].

These are only some technological trends, among the many that use data-harnessing concepts, often labelled as 'Smart'. Due to their ubiquity, we can only expect similar examples to become more and more popular.

Smart Buildings

Today, the notion of Smart Cities is popular, profitable and academically thriving. The underlying notion that a proliferation of connectable infrastructure, distributed, personal sensors and big data could create efficient, enjoyable and sustainable cities has become one of the defining schemes of the current age [170][172][173].

The application of the same notions and fundamentals within the bounds of a building instead of the whole city (i.e. Smart Buildings) has a relatively smaller growth although it is actually an essential part of the applications in a city level [174].

At the Barcelona Smart Cities Expo 2014, a Cisco representative suggested that buildings had 'locked the doors' to the widespread interest and awareness of intelligent, integrated data-based solutions that were sweeping the cities of the world outside, missing out on a significant amount of potential value [175].

The existing work in the field of Smart Buildings, research tends to be more aligned with more traditional concepts such as 'smart energy', 'smart structures', 'smart lighting' etc.

Hot-Desking Background

After the rise of the service sector in developed western economies, new large office workplaces were built by a new and increasingly diverse wave of consultancies and financial services. This, in conjunction with the rising rental costs in the large cities where these offices needed to be located [176], generated the issue of excessively high real estate costs for the companies.

As such, minimising the cost of large office areas became increasingly important. A popular idea emerged in the late 90s to replace territorial working systems - whereby each individual is directly associated with a specific desk - with an allocation system whereby those who attend the office on a specific day are given a free desk from a pool. The key value driver of this was that office sizes could be reduced up to 30% [177] depending on the tendency of the business to visit clients and collaborators outside the premises. A rise in part-time working further improved the benefit of non-territorial desk systems [178].

Today, the form of Hot-Desking that is usually met is simply employee-led: on attendance to the workspace, an employee chooses a free desk and claims it for the day. However, such schemes have had mixed success [76]. Literature's criticisms on that can be categorised into three key aspects: (a) Ineffective management applying slow and inconsistent methods of distributing desks that can often even lead to misunderstandings about whether or not a desk if free [77], (b) Loss of working synergies which actually consists of the loss of collaboration and exchange of ideas due to not placing staff working on similar projects in close proximity, and (c) cultural and behavioural barriers which could include but not limited to the personalisation of an office (which is mostly lost in Hot-Desking environments) that could make the individual more comfortable and therefore more productive [79]. None of these parameters should look insignificant since even small variations (for example 1% decrease) in productivity can have significant impact on even the smallest scales [78].

Intelligent Hot-Desking

The rise of 'smart' enablers provides a unique opportunity to fundamentally alter the nature of Hot-Desking by utilising increased data about the workplace, its occupants and their intentions and preferences. There is a considerable literature base that highlights that an employee's position, both in an absolute sense and in relation to other employees, has a strong impact on their behaviour and happiness in the workplace [86]. In principle, rather than a 'pegs into a slot' approach (i.e. simple linear desks assignment in a first-come-first-served basis), intelligent Hot-Desking would evaluate the best position for an employee to work based on an algorithm combining a number of weighted inputs. These inputs could include, but are not limited to:

Noise levels of workplaces derived from acoustic sensors distributed across the office. There are workgroups that due to their work subject can only tolerate minimum noise (and usually produce minimum noise too) while other groups can work effectively in a noisy environment as well. The inability to effectively manage noise-sensitive and noise-making workgroups in an office can be one of the top 3 factors preventing their company from being more profitable. [84][179]

Duration of stay, derived from calendar data or asked for at an on-arrival desk request. Smaller ‘touch down desks’ can be useful for individuals staying for exceptionally short periods of time. This may further improve the floor area savings of traditional Hot-Desking.

Nature of work, which in the case of a very large staff group, could be derived from a system, where keywords for the type and project of work could be requested from individuals for a given day or calendar period. This element will enable workgroups of individuals with similar subjects and possibly similar goals to be formed which is proven to lead in greater productivity. Similar benefits would be realised for smaller projects, too. [83]

Environmental preferences derived from various datasets, that could be generated, among others, from temperature and light sensors across the office. Many small but psychologically significant issues could be tackled this way. For example, individuals with a preference to warmer office environments could be placed further away from colder areas, whereas those with a mood that is more influenced from daylight on could be placed closer to the window.[86]

Desk configuration derived from asset location and management information and could include office equipment such as multiple monitors etc.

There could also be other kinds of personal preferences that could be, derived from occupant feedback (like for example level of satisfaction about previous desks given). Of course, the most appropriate combination of all the aforementioned parameters will always be heavily context-dependent.

Purpose

While it is apparent from the outset that distributing desks intelligently is indeed possible, little research exists on how optimization might look in practice, or the value it could bring to the workplace. This is a significant lack, especially considering that intelligent Hot-Desking cannot only increase the productivity within the office premises, but also decrease the rental costs, which can sometimes be up to 10% of the total cost of the company [89].

Within this study we will explore the potential for Intelligent Hot-Desking to result in superior working conditions (in the form of increased productivity) in comparison to Traditional Hot-Desking Systems.

To demonstrate this, we will use the distribution logic of 'work theme' within a demonstrator context of an engineering consultancy's commercial office, facilitated by primary data.

As such our objectives are as follows:

1) Establish a modelling framework, context and distribution algorithm for our scenario.
2) Observe the practical workings of an Intelligent Hot-Desking System throughout a simulated day.
3) Deduce an estimate for the improvement in productivity that Intelligent Hot-Desking Systems could bring over Traditional Hot-Desking Systems.
4) Discuss the potential barriers and enablers to implementation of Intelligent Hot-Desking Systems.
5) Explore the potential for expanding the model to inter-organisational scenarios and professional social networks.

4.3.2 Intelligent Hot-Desking Model

The content of this section addresses part of RQ3 by thoroughly presenting our Intelligent Hot-Desking approach and explaining how it improves the existing literature and its benefits over traditional Hot-desking.

This section will detail the approach followed in order to test the concept of Intelligent Hot-Desking. This entails:

- Optimisation Selection: consideration of the type of data and corresponding mechanism of value creation that will be the focus for testing the concept;
- Detailed design: the specific assumptions and model design in translating the real-world environment to the digital model;

- Value proposition: the approach of assessing any value that is created;
- Intelligent Hot-Desking Distribution Process: the specific approach of implementing the mechanism of value creation;
- Comparison Cases: consideration of base cases for reference points when assessing value created;

Optimisation Selection

To test the concept of Intelligent Hot-Desking, a distribution logic of just one data type will be used for simplicity. After analysis of all of the potential distribution types that have been identified in the literature review, the distribution logic of 'work theme' has been chosen. This has been selected for the following reasoning:

- It is relatively easy to collect primary data on employee's typical work-type patterns, compared to more complex datasets such as noise generation.
- It works around a hypothesis of creating 'positive' working benefit, rather than avoiding 'negative' working obstacles. It is believed that this will be applicable to more real-life contexts.
- In theory all employees of the office are influenced by such a distribution logic, on the logic that all have work of a certain type.
- Placing employees based on the work-type may also indirectly take into account their noise level needs.

The scenario context we will be emulating will be based on primary data provided by an engineering consultancy in the UK with an office in the city of London. By observation and interview, this is perceived to be an office that bears many similarities to the majority of offices for medium and large organizations.

The scenario will be modelled by a discrete events simulator focusing on the office as a number of desks; each of which either has an individual in or not. Each individual will have characteristics, some of which are input (relating to their intentions) and some others are output (relating to how their working environment has influenced them). These are defined in the following section.

On arrival, an algorithm will decide the place for an individual to sit. While an individual is in a desk, for every unit time that progresses, the environment will be assessed, through a methodology defined in the section about value proposition. The simulation will run for 1 day, with one-minute clock pulses. The productivity values for each person will be summed each second, for the day, giving a selection of overall 'scores' for a given allocation system.

This process will run for a selection of distributions of Intelligent and 'Traditional' Hot-Desking for the purposes of comparison, detailed in the corresponding sections where the intelligent Hot-Desking distribution process and the comparison cases are described.

Detailed Design

The behaviour of individuals will be based on primary data including observational data, security 'swipe gate' data and interviews with office occupants. Based on these, the scenario has been given the following characteristics:

Office grid: 12 x 12 desks
Total daily employees: 155

The employees are more than the offices since, as discussed, one of the benefits of Hot-Desking is to cut down on costs by not having as many desks as there are employees.

It was observed in our primary data that the time spent in the office will vary distinctly between individuals. Support staff, such as HR and Accounting are unlikely to ever leave for off-site work. Low and middle-ranking general employees are likely to attend client sites on occasion, and high-ranking staff, whose role include client relation management and thought-leadership, are likely to regularly leave, and be, out of office. These are generalisations that are being made on one specific primary data on a specific context, and the exact spread and nature of office attendance will depend on organisational size, office size, industry and organisational culture. As such, for the

purposes of this model we will generalize to an 'average' staff member based on our primary data.

By observation of the primary data - specifically the swipe gate records - from the office, the flow in to and out of the office in this scenario is a combination of:

i. Traditional morning and evening peaks for entrance and exiting to the office.
ii. Between these, a lesser, broader flow of assorted leaving and re-entering of the office for various business engagements. The leaving is centred around before lunch (12:30-13:30), the arriving centred after lunch.

The first is relatively easy to simplify for repeatability in the model; the latter will require considerable simplification. Fitting normal distributions by observational trial and error, this model will estimate the probability of an individual entering the office over the course of the day and the probability of an individual who is in the office, leaving an office, as the sum of the following weighted distributions:

- $Arriving: w1 * A + w2 * B,\ w1 + w2 = 1$
  - $A: Norm(8.5\ , 1),\ w1 = 0.7$
  - $B: Norm(13\ , 5),\ w2 = 0.3$
- $Leaving: y1 * A + y2 * B,\ y1 + y2 = 1$
  - $A: Norm(18\ , 1),\ w1 = 0.7$
  - $B: Norm(13\ , 5),\ w2 = 0.3$

(52)

Figure 51: Arrival and Leaving probability distributions

Figure 51 displays this graphically. These estimates will serve as a reasonable assumption for a generic context – variation will exist between different companies and different industries so accuracy beyond this is excessive.

A simplification will also be made as to there being no interrelation between comings and goings of individuals; if an individual arrives late to the office, they are just as likely to leave for a meeting as they are as someone who has been there since early. Furthermore, employees will only be able to enter and leave the premises once. The probability distributions will in effect simulate real return visits as new individuals.

Lunch and other temporary breaks have been ignored as observation demonstrates that desks remain allocated during these periods. In addition, individuals may not have to swipe their card when going for lunch.

The distributions of work-types in the primary data are:

Type A: 0.4, Type B: 0.3, Type C: 0.15, Type D: 0.1, Type E: 0.05

Indeed, while this specific distribution may not be the reality in all samples, interviews conducted suggest this is not unusual for the industry from which the examined organisation is from, although the level of segmentation in ‘work theme’ is highly open to interpretation.

Value Proposition

To evaluate the potential of Intelligent Hot-Desking a framework for assessing the value of this distribution over a traditional Hot-Desking system must be defined. As mentioned previously, the literature has demonstrated that Hot-Desking overall can save rental and operational costs through a smaller floor area and brings improvement to the 'wellbeing', 'happiness' and 'effectiveness' of individuals. In terms of considering which can be quantified with the most validity we concluded at 'effectiveness'. For simplicity, we will perceive being 'effective' as one's ability to complete their purpose in the office environment, which we will simplify in turn as the 'productivity' of an individual in the office.

As discussed, research has simply shown that the quality, with respect to pragmatic business ends, appears to be higher when 'the right' individuals are in a 'close proximity'. In particular, the ability to speak to one another is regularly cited as a beneficial consequence of sitting near another individual [174]. In our research, we assume that employees working at the same work-group will benefit each other (i.e. will improve their productivity) if they sit close to each other, due to the interaction and communication developed. Thus, we will use the behaviour of noise to model these interactions since noise levels can determine the quality of the aforementioned communication.

For that, we consider employees of the same workgroup of being able to have a positive impact on each other when in close proximity; impact that will follow a square law decay. Since this impact only depends on the workgroup that they belong and their distance, we have that the influence of employee i on employee j is equal to the influence of employee j on employee i. Of course, every employee will benefit from each colleague of the same group, thus the total influence on an employee is the sum of all these influences. We model irrelevant employees (the ones that do not belong to the same workgroup) as having no impact on each other.

Units are assumed to have a size of 2.5m boundary from observation and noise is considered to be measured 0.5m from the centre of the unit – again, a realistic point of seat. We will then use basic square law as an estimate:

$$I_2 = \left(\frac{d_1}{d_2}\right)^2 \times I_1, I_3 = \left(\frac{d_1}{d_3}\right)^2 \times I_1 \quad (53)$$

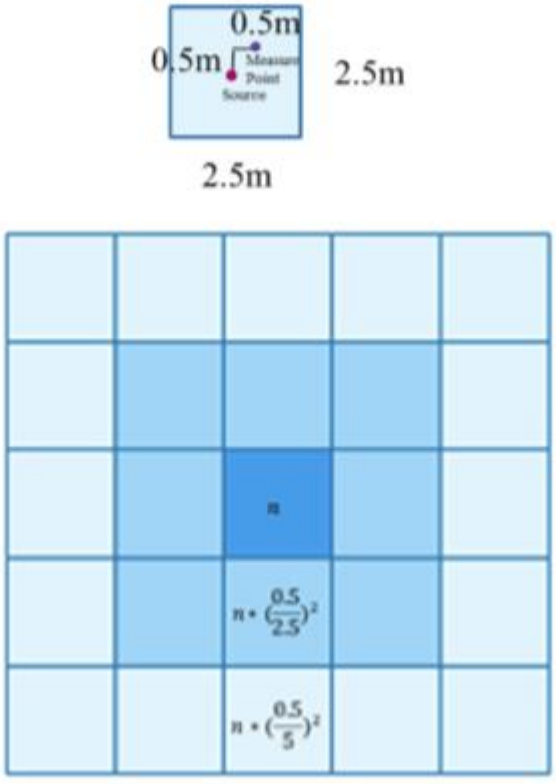


Figure 52: Propagation of positive work theme environment

For simplicity, diagonal inaccuracies will be ignored. Value of n will start at 25, and according to Figure 52 and formula (53), will produce a value of 1 for individuals in the closest possible proximity – the immediate row and 0.25 for the row next to it. Further rows are neglected for simplicity.

In other words:

2nd Row: 0.25

3rd Row Onwards: (negligible, neglected for simplicity)

This means that every employee has a productivity equal to zero when arriving at the premises. The algorithm then assigns a desk to each one of them and each one's productivity becomes equal to:

$$Prod(emp) = 1 \times k_1 + 0.25 \times k_2 \quad (54)$$

where, k_1 is the number of employees that occupy desks (out of the 8 in total) directly neighbouring to the employee whose productivity we measure (i.e. first row neighbours) and belong to the same workgroup and k_2 is the number of employees that occupy desks (out of the 16 in total) that are next to the first row neighbours of the employee whose productivity we measure (i.e. second row neighbours) and belong to the same workgroup.

It can be easily observed that if all first-row neighbours are of the same workgroup, a productivity of 8 (8x1) is achieved. If this is the case for the second-row neighbours as well, then a value of 12 is achieved (8x1+16x0.25), which is the maximum achievable productivity for any individual. Therefore, there is obviously a synergy that is developed among individuals of the same workgroup since they improve each other's productivity. Based on this way of calculating an employee's productivity, the Hot-Desking algorithm will assign to an incoming employee the desk that will increase the total productivity of the offices (which is the sum of the productivities of all the employees) as much as possible. If the incoming employee is not possible to sit next to the employees of the same workgroup, then the total will remain the same. In general, the productivity can only decrease when an employee leaves the premises.

According to formula (54), the productivity of any individual is equal to zero when there is no one of the same workgroup at the next two rows (initial productivity). That does not mean, that this individual is not productive at all or that is not contributing at all to the company. However, since this model's goal is to allocate employees to desks in a way that the total productivity is as high as possible, we would still get the same optimal solution even if we assumed that their initial productivity is not equal to zero. For example, setting initial productivity for employee i equal to $prod_i$ and comparing between two possible allocations, U_1 and U_2, of a number of employees where c among them do not have any neighbours of the same workgroup, then assuming initial zero productivities we would have:

$$Productivity\ (U1) = P1\ and\ Productivity(U2) = P2 \quad (55)$$

and with the adoption of $prod_i$, we would have:

$$NewProductivity(U_1) = P_1 + prod_1 + prod_2 + \cdots + prod_c$$

$$NewProductivity(U_2) = P_2 + prod_1 + prod_2 + \cdots + prod_c \quad (56)$$

Thus, the result of the comparison between *Productivity(U_1)* and *Productivity(U_2)* would, obviously, be always the same as the result of the comparison between *NewProductivity(U_1)* and *NewProductivity(U_2).*

Intelligent Hot-Desking Distribution Process

There are several methods by which the allocation of the desks among the employees could be evaluated. These include:

Method 1: On-arrival, current-state individual optimisation – In a system where no information is given in advance about who will be in and who shall not, each seat is allocated in a way that will maximise the benefits (in this case the productivity) of the arriving individual at the exact moment they enter.

Method 2: On-arrival, current-state group optimisation – In a system where no information is given in advance about who will be in and who shall not, each seat is allocated in a way that will maximise the benefits (in this case the productivity) of the whole office at the exact moment a new attendee arrives.

Method 3: Full-term, group optimisation – In a system where information is indeed given in advance about who will and will not be in (including duration of stay), each seat a way that will maximise the net conditions for all individuals intending to arrive that day, considering all permutations of seating across the entire day.

It is clear from basic experimentation that the more advanced the system is, the more optimal the seating allocations and the higher the net gain will be overall.

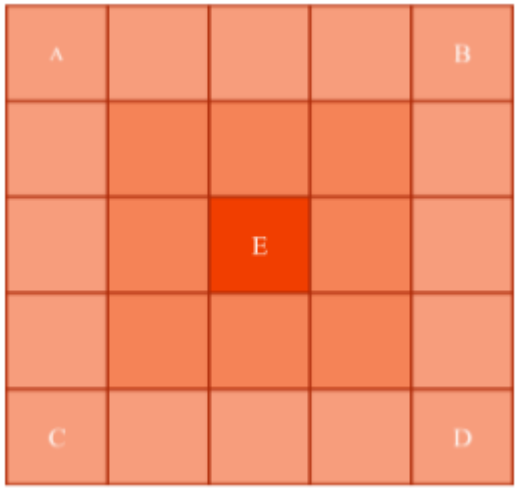


Figure 53: Tie-breaker distribution logic

In order to avoid reviewing an allocation process with significant barriers to implementation (Method 3 which requires the supply of additional staff data in advance), Method 2 will be utilised.

It can be observed that with Methods 1 and 2, many desk allocations will be equally optimal, especially at the beginning of the day – yet their decision will strongly affect the rest of the day. As such a tie-breaker rule is required.

After experimentation of several tie-breaker systems, the most effective was settled upon. When there is no difference in the effectiveness of the allocation, the system will attempt to send an employee with a specific work-type as close to a predefined extremity of the office that has been preassigned to that work-type. In our case, these will be the four corners of the office grid along with its centre desk (Figure 53). In this way, the allocation process has a disposition to form colonies when no better allocation logic is available. Based on the aforementioned logic, this will have a positive impact on the overall productivity of the employees since the creation of colonies will attempt to partition the office grid among the workgroups pre-emptively.

Comparison Cases

For the purposes of developing a reference point for comparison, three 'less intelligent' scenarios will be prepared:

i. Individuals come in and are allocated a desk at random from free desks, with no logic applied.
ii. Individuals come in and are given a desk in a 'closest desk free' (to the top left of the office) system. Essentially, this is the linear, 'pegs into a slot' distribution that has already been discussed.
iii. For means of understanding its influence, a distribution that simply has the 'extremities' tie-breaker logic only and aims to place individuals as close to the predefined extremities without the evaluation of the intelligent system.

Results

The below outputs are displaying the office state at specific time 'slices' throughout the day.

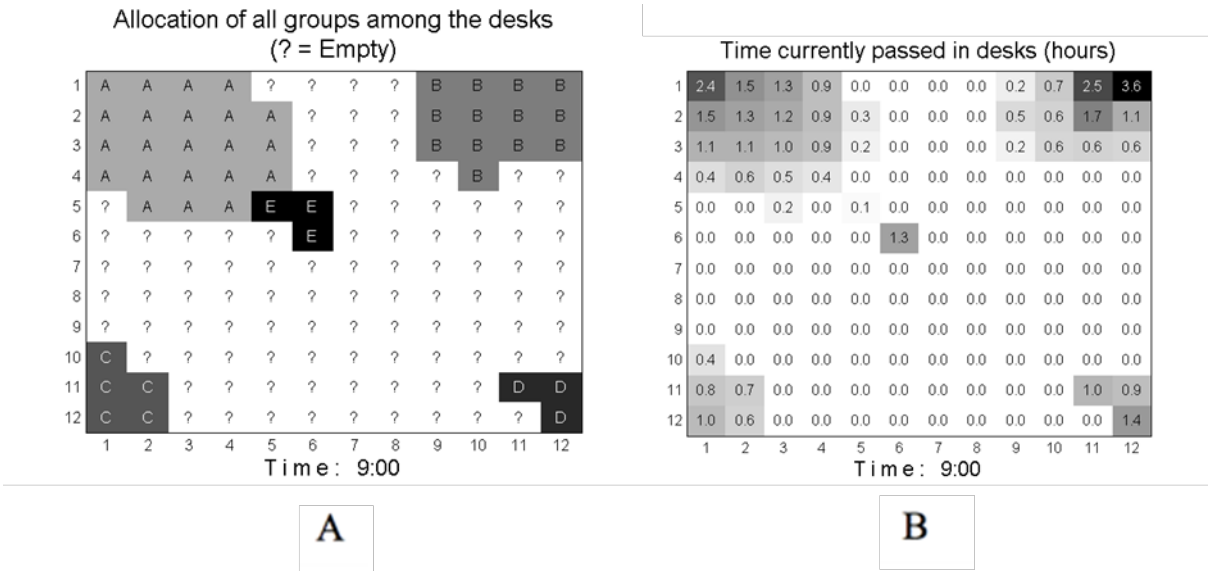


Figure 54: Snapshot of A) all groups' allocation among desks and B) time spent by employees in their desks

The first diagram, seen in Figure 54(A) is a graphical representation of the position of different work themed individuals, labelled and shaded by their work theme, or an empty office space, designated by '?'.

Figure 54(B) demonstrates the duration an individual has been at the desk. Note that all times are rounded to 1 decimal number, so zero does not necessarily specify an empty desk. In this figure and the similar to this below, the darker a 'desk' is, the higher the number on the figure for this particular desk.

The following time snapshots were taken for different times throughout the day.

Snapshots at 11am

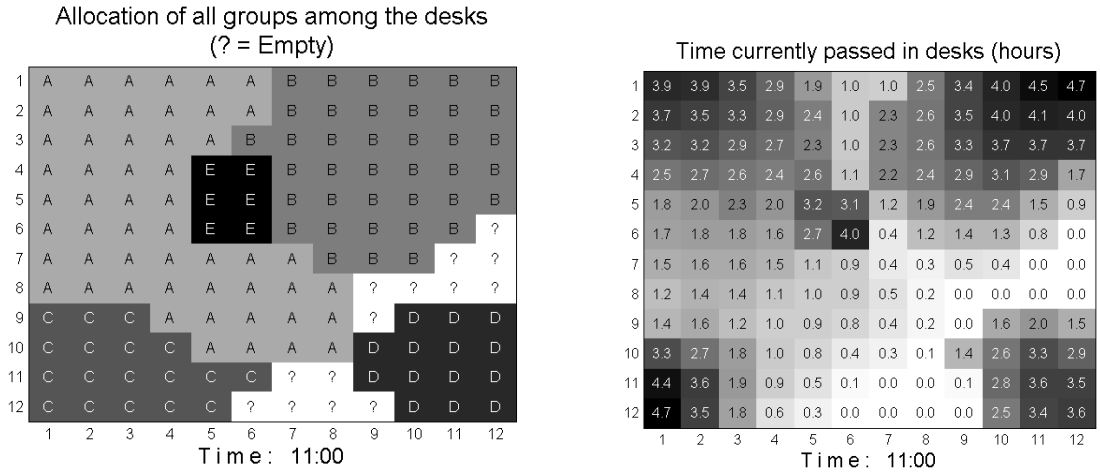


Figure 55: Snapshots at 11am

Snapshots at 1pm

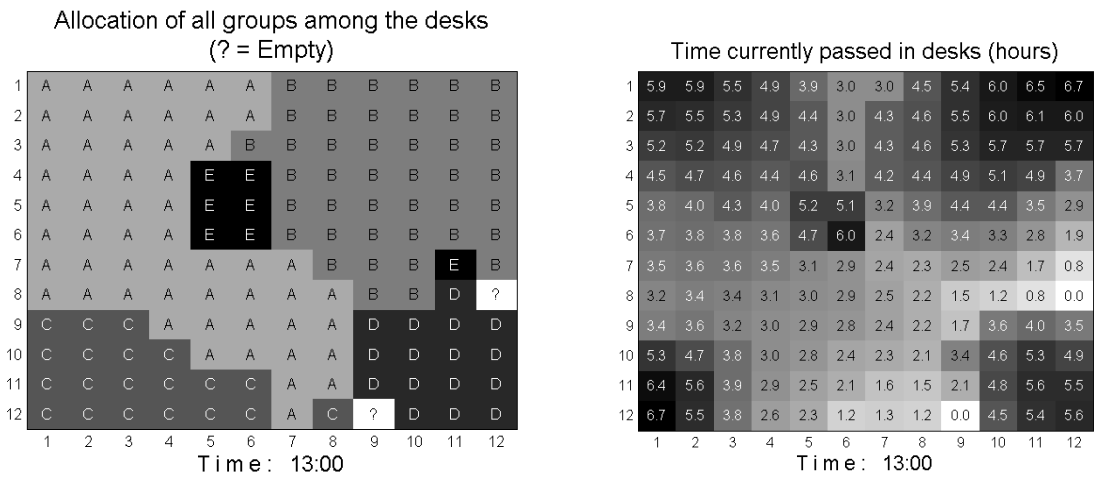


Figure 56: Snapshots at 1pm

Snapshots at 2pm

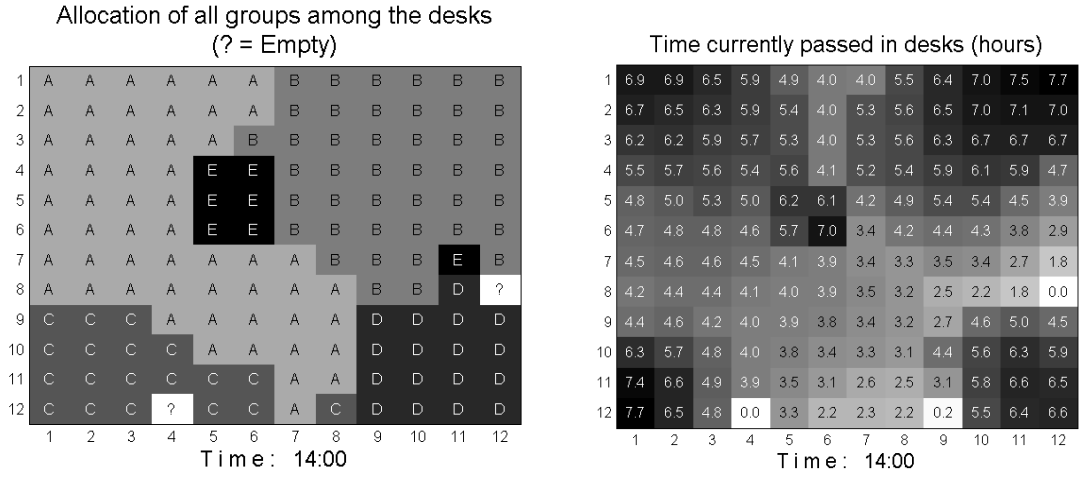


Figure 57: Snapshots at 2pm

Snapshots at 3pm

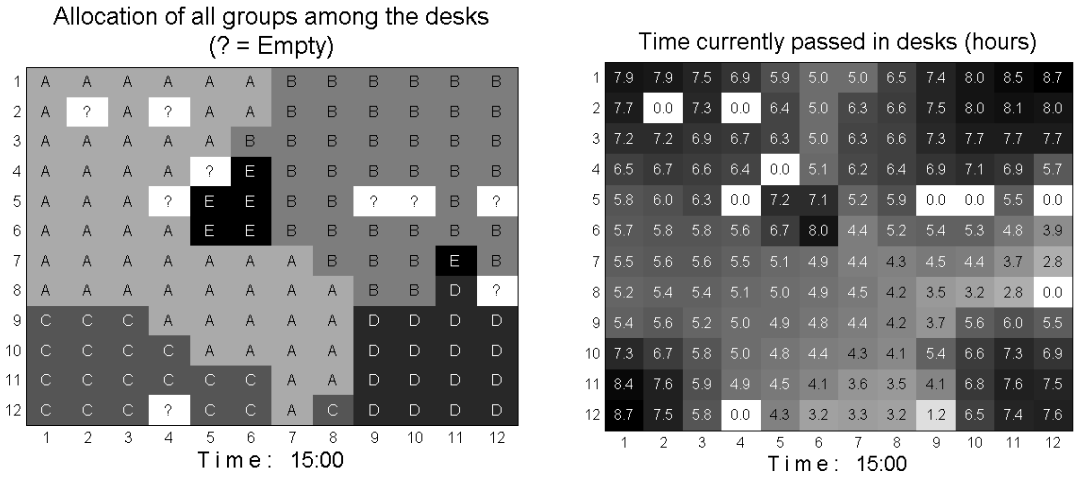


Figure 58: Snapshots at 3pm

Snapshots at 4pm

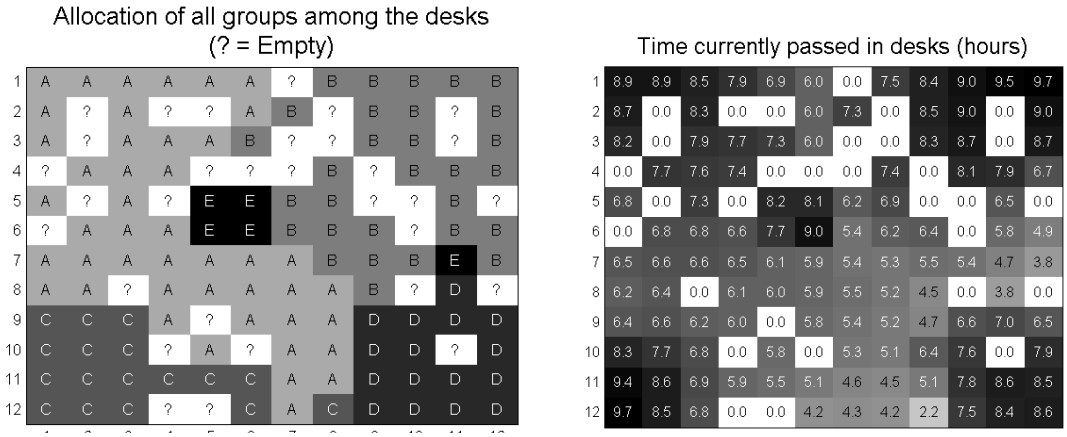


Figure 59: Snapshots at 4pm

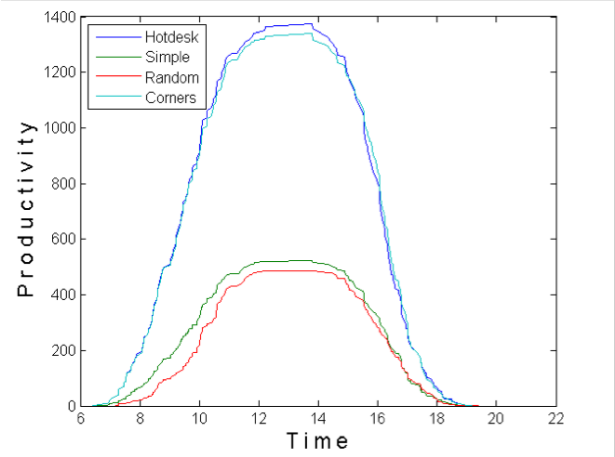


Figure 60: Total Value Proposition Framework Output by distribution method

The summed productivities of all individuals in the office by the Intelligent Hot-Desking System ("Hotdesk"), Comparison Case 1 ("Random"), Comparison Case 2 ("Simple") and Comparison Case 3 ("Corners") can be seen, as time goes by, in Figure 60.

Observations

Compared to either of the traditional Hot-Desking results it appears that over the core hours of the day, the system of allocation has produced approximately 2.8 times the improvement of seating location – using the relative metric - over the two traditional methods of desk allocation.

Additionally, it can be observed in the scenario from Figure 60 that the influence of the tie-breaker logic is extreme.

By 11am when the majority of the am peak has entered, the office is at a high occupancy and there has been little exiting of the workforce. By 2pm, as some individuals leave and others attend, it can be observed that the algorithm is making decisions between several sub-optimal configurations and improving over the extremities system. By 4pm, the office is sufficiently clearing out from the beginning of the PM peak that when new entrants arrive, there is a high probability of a reasonable desk choice being a distributed extremity, so again, the intelligent algorithm loses advantage although it is not

outperformed by the "corners" variation. An increase in the number of work groups, which is a very possible real-world situation, would also favour the more intelligent distribution.

Additional variations

Now that we have concluded which one of the four Hot-Desking logics is performing better (i.e. leads to a distribution of employees with higher total productivity than the total productivity of the distribution that the remaining three variations lead to - Figure 60), we are going to examine four different variations of this logic. All four variations are the following:

Model 1: When an employee arrives, the algorithm assigns an empty desk to them. If there is no free desk, the employee leaves the premises and does not return the same day. When the employees leave the premises, either because it is time for them to leave or because there is no free desk, they do not return the same day.

Model 2: When an employee arrives, the algorithm assigns an empty desk to them. If there is no free desk, the employee goes at the end of a First-In-First-Out queue. The employee leaves the queue if it is time to leave the premises or if there is a free desk for them (whichever comes first). When the employees leave the premises, either because it is time for them to leave or because there is no free desk (or both), they do not return the same day.

Model 3: When an employee arrives or when an employee departs, all the employees (apart from the one that is leaving, in the case of departure) are reassigned (possibly differently) desks of the grid, so that the maximum possible productivity can be achieved with the given employees at that time. When an employee arrives and there are no free desks, the employee leaves the premises. When the employees leave the premises, either because it is time for them to leave or because there is no free desk, they do not return the same day.

Model 4: When an employee arrives or when an employee departs, all the employees (apart from the one that is leaving, in the case of departure) are reassigned (possibly different) desks of the grid, so that the maximum possible productivity can be achieved with the given employees at that time. When an employee arrives and there are

no free desks, the employee goes at the end of a First-In-First-Out queue. The employee leaves the queue if it is time to leave the premises or if there is a free desk for them (whichever comes first). When the employees leave the premises, either because it is time for them to leave or because there is no free desk (or both), they do not return the same day.

It is worth clarifying that an employee can leave the premises while waiting in the queue, for the same reasons that they could leave while being in a desk (i.e. external business commitments etc.). Model 1 is the one that prevailed before.

The aim of these extra variations is to take that previous part of the study one step further and compare Model 1 with variations like Model 2, Model 3 and Model 4. Although it is obvious that Model 3 and Model 4 are not applicable in real life, they are still useful for comparison because they represent the ideal models. That is because these two models solve an inevitable problem that Model 1 and Model 2 have. Although Model 1 encourages the creation of colonies by employees from workgroups A, B, C, D and E (which is the best way to result in a high total productivity since individuals increase their productivity when they are close to other individuals of the same workgroup), inevitably there will be times where a colony will have a free desk in it, due to a departed employee of that colony, which will be occupied by an employee of another workgroup who cannot be placed closer to their own workgroup because there are not any free desks close to that group. That will create desk grids with individuals that are not placed in the most optimised way. However, this is inevitable unless all employees are rearranged frequently during the day, which is impractical and inapplicable in real life. It is useful though to check how much better the results of Model 3 and Model 4 are when compared to Model 1 and Model 2 respectively, because if the difference is small that would mean that Model 1 and Model 2 are actually very close to the absolute optimal and therefore work great.

New Results

The impact of all models on the total productivity of the organisation throughout the whole day, is depicted in Figure 61.

The equivalence of the aforementioned models to the ones on Figure 61 is: Model 1 = Hotdesk, Model 2 = Queue, Model 3 = New and Model 4 = NewQueue. Judging by

this figure, we can tell that the addition of queues not only has very small impact on the productivity, but also that slight impact is not always positive (it is not easily visible in this size of the figure but it is positive sometimes) and it can also be negative. That may not always be the case with queues, but even in this case it should not be seen as an unorthodox fact. The reasoning behind that phenomenon can be explained with the following example. Since the employees are less than the desks, there can be times where all desks are occupied and employees keep arriving. In the scenario that includes queues, if employee e1 arrives and there are no free desks, e1 will go last in the queue. If employee e2 arrives later and there are still no free desks, e2 will go last in the queue, behind e1 (providing that e1 has not left the queue because it was time to leave). By the time there is a free desk for e2, it can be the case that e2 has already left while some other employees, like e1 for example, may have found a desk by then. Therefore, due to the queues, employee e1 was advantaged compared to e2. However, if there were no queues, there would be higher chances for e2 to find a desk on arrival because if some other employee, like e1, had arrived before e2 and had not found a free desk, they would have left, instead of waiting in a queue in front of e2. Thus, in the case of queues, e2 would be disadvantaged compared to e1 even if e2 had more to offer than e1 to the total productivity. This example demonstrates situations that can occur and lead to Model 2 resulting in less productivity than Model 1 (and Model 4 less than Model 3, respectively) for some periods of time. To sum up, queues maintain the first-come-first-served logic of the desks assignment whereas absence of queues can break that rule (like in the example where e2 could have found a desk before e1, if e1 had departed just after their arrival) which can sometimes be beneficial for the total productivity.

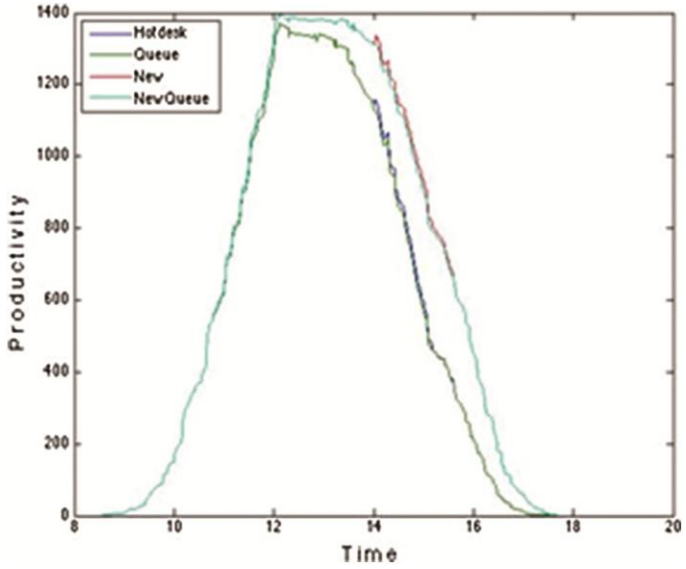


Figure 61: Comparison of all 4 models with respect to the productivity they result in

However, the most important finding that comes out of this figure is the fact that Models 3 and 4 do not produce significantly better total productivity than Models 1 and 2, respectively, throughout the biggest part of the day. In other words, the, not applicable in real life, Models 3 and 4 that produce the best possible total productivity, seem to perform only slightly better than Models 1 and 2, respectively. The only periods of time, that Models 3 and 4 outperform Models 1 and 2 significantly is towards the end of the day when not many employees are still at their desks and if they have been arranged according to Models 1 or 2 then they will most probably be disorderly spread. And still, this difference is significant, more in percentage terms and less in absolute numbers That is a huge success for Models 1 and 2 and a very good indicator that there is not much room for improvement of the algorithm, providing that the fundamental assumptions of the model remain the same. A possible and simple way to make Model 1 (resp. Model 2) almost equivalent to Model 3 (resp. Model 4) is to rearrange all employees only once (which is viable) in the afternoon, when the impact of the many departures is already apparent. After that time, although Models 3 and 4 will continue to perform better than 1 and 2, the difference will be even smaller. Figure 62 actually demonstrates that idea in practice for Model 1 (‘Hotdesk’) compared to Model 3 (‘New’). The reassignment occurs at 3pm and its result is demonstrated on Figure 63.

In order for the difference between Model 1 and Model 3 to be seen in practice, snapshots from the distribution of employees among the desks is provided at 3 pm, when a significant amount of employees has already departed and since there are not many that are still to come, most of the workgroups are not optimally spread across the desks, in case of Model 1, but are still optimally spread in case of Model 3. This is not a contradiction to the previous explanation of Figure 63 because it is expected that the snapshot at 3 pm of the modified version of Model 1 (with one rearrangement at 3 pm) will be the same as the snapshot of Model 3, at the same time (3 pm).

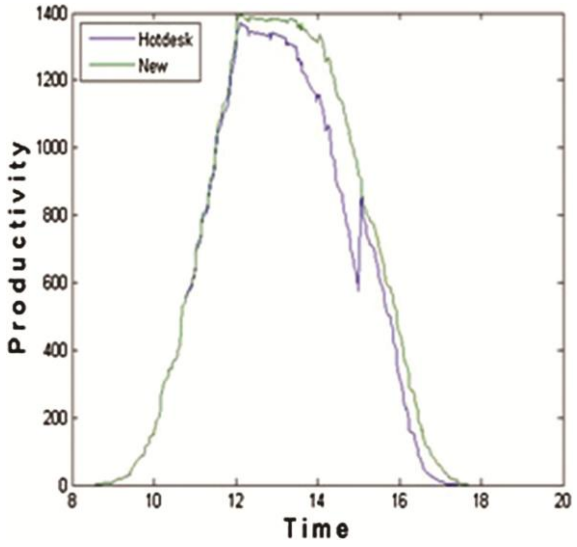


Figure 62: Comparison of Model 1 with a rearrangement at 3 pm ('Hotdesk') to Model 3 ('New')

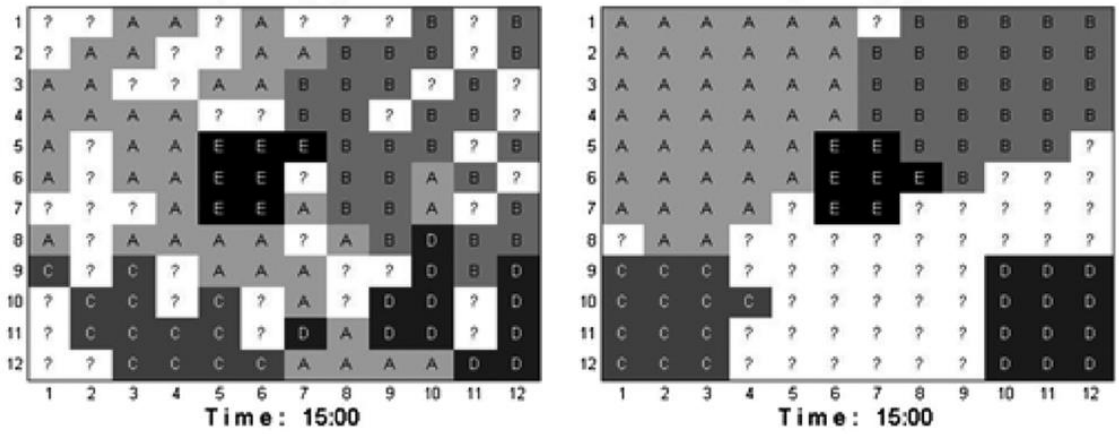


Figure 63: Snapshots of workgroups allocation for Model 1 (left) and Model 3 (right) after reassignment at 3 pm (? = Free)

Cost of System / Productivity Improvement	£ 3,750	£ 7,500	£ 15,000	£ 30,000	£ 60,000	£ 120,000
0.1%	1.2	2.4	4.8	9.7	19.4	38.7
0.5%	0.2	0.5	1.0	1.9	3.9	7.7
1.0%	0.1	0.2	0.5	1.0	1.9	3.9
5.0%	0.0	0.0	0.1	0.2	0.4	0.8

Figure 64: Payback time, in years, of an implemented system within the scenario office, at varying productivity and cost levels.

A sensitivity analysis of payback years for the adoption of this Hot-desking sustem can be seen in Figure 64. Based on interviews, an office improvement that pays back within 10 years is generally viewed favourably, which means the scenario system would be viewed as a positive investment in all but the most conservative of scenarios. It is also worth mentioning that a cost around £15,000 is considered realistic enough [180]

Barriers and Enablers

The following consideration of barriers and enablers is derived from a combination of interviews, observations from the modelling above and literature review.

Considering practicalities, Method 2, the distribution logic chosen here, may actually be the best possible distribution method for an office manager, if they do not have the capability or do not wish to bring about the cultural change of specifying office

attendance in advance. It is difficult to imagine a scenario where Method 1 would be preferred to Method 2 as the difference in processing complexity is minor for what is perceived to be substantial improvement.

The popularity of Intelligent Hot-Desking systems in commercial office contexts will depend heavily on the business and industry in question. Level of suitability may well mirror those typical of traditional Hot-Desking - where the cost of labour is high in relation to real estate costs and are likely to favour maintaining a territorial working environment. However, there may be interesting niches within high-wage industries where concepts - such as 100% staffing models experiencing growing popularity in strategy consulting and product design - may favour project-based allocation. Furthermore, the more of these workgroups there are or the smaller they are defined to be, the more valuable the intelligent distributions will get.

Considering the cost of implementing the sensing for such a system, it is notable that this infrastructure may be shared across a number of other Smart Building use cases, thus improving the return on investment further.

Related to this, broadening the boundary of analysis further, regardless of the data type upon which distribution takes place, a significant source of value in Intelligent Hot-Desking comes from the reusability of the occupancy data it creates. There are many possible incarnations of this.

One example would be the consideration of a real estate strategy. Rich occupancy data could allow analysis of the future real estate requirements of large, multi-office commercial entities at minor cost; a procedure otherwise slow and expensive [181]. Considering the market in different sectors, anonymised occupancy data could be sold externally to be used by taxi companies who are interested in rapidly detecting and capturing the trade associated with those leaving commercial buildings at unexpected times. As another example, the occupancy data of buildings could be used to adjust the routing or schedule of nearby public transport services in real time.

Finally, and more specifically to Intelligent Hot-Desking rather than occupancy data, this concept could help to facilitate short term office hire. Through user-recognition, these systems can not only simplify the payment for per- desk-per-hour real estate models, but also ensure these highly diverse office communities are structured in a logical way.

Findings and Conclusions

Out of the three methodologies that were described earlier (i.e. (a) On-arrival, current-state individual optimisation, (b) On-arrival, current-state group optimisation and (c) Full-term, group optimisation), we modelled the second one. That is because it is more sophisticated than the first methodology and there are only specific applications where this could potentially be preferred. The third methodology would require even more data and forecasting on the arrival and departure times which means that there would be the danger of resulting in big inaccuracies. Furthermore, an adjustment period is required before such a model can be trusted. Using the second methodology we managed to provide a realistic and productivity-oriented way of assigning desks to individuals at a workplace and not only did we confirm that this method can outperform other common ways of desk assignment, but we demonstrated that its effectiveness is comparable with an impractical model that was designed to result in the optimal outcome. Furthermore, the profit implications for the corresponding organisation were analysed and the adoption of the model was found to be an easily repayable investment.

Ultimately, intelligent Hot-Desking appears to have the potential to bring about transformative change in the commercial office workplace backed by a strong value case. The exact value such schemes bring however, will be highly-dependent on the type and methodology of implementations, and it is the opinion of this work that significant research needs to be undertaken on this topic. Primary research in the form of experimentation and observation, to better understand the specific productivity benefit, would be highly influential in drawing in industrial interest.

This whole work can be used for greater social impact that transcends organisational boundaries. At the heart of it, is the assumption that sensing data and personal preferences can be fed into an intelligent platform that will bring together the most suitable co-workers under their preferred working conditions. But there is no constraint to assume that these persons must be working within the same organisation. In fact, if we apply this model in facilitating the desk allocation in the scenario of a business incubator, it could bring together complementary skills and expertise as well as personality types. To that effect, this model could be developed further to include inputs related to more parameters (e.g. social media updates), besides the ‘hard’ sensing data

which may include e.g. presence and location, as well as predefined personal preferences (like noise and environmental conditions) and maybe calendar entries, as well leading in multi-dimensional optimization.

4.4 Conclusion

All in all, in this chapter, our resilience-oriented contribution is presented through the corresponding use cases. These use cases include models that apply on WSNs (approaches combining Game Theory and SensomaX) and EDS on Hot-Desking. As a result, the identified gaps of the existing approaches have been mitigated and RQ3 has been answered.

III. CONCLUSIONS AND FURTHER WORK

Section II, the last section of the thesis, includes Chapter 5; the chapter that concludes the research conducted. In particular, it summarises this work's findings and research contribution, discusses how and where exactly in this thesis the research questions have been addressed and concludes the whole thesis.

5 Chapter

CONCLUSIONS AND FURTHER WORK

Chapter 5 summarises the research contribution and discusses the findings of this work. As such, it provides the outputs and summary of the two focused areas and how they have been delivered, improving the security and/or the risk management procedures as well as improving the resilience (in this context meaning any system's aspect that is not security-oriented) of the systems. Finally, it discusses the research questions of this thesis and the way they have been addressed.

5. Conclusions and Further Work

5.1 Summary of Contribution and Future Work

This thesis covers many different use cases. Therefore, for better understanding, this section will include each use case's summary of findings and conclusion, instead of just one attempting to cover them all.

5.1.1 Security and Risk Management

Starting with the part of the research that focused on improving the security or the risk management procedures of different kinds of systems, we firstly have the proposition of an IDS and an IPS that can be applied on a WSN in order to help the network operators make automated decisions regarding the trustworthiness of the data that their WSN produces. In particular, the proposed IDS and IPS were able to suggest to the network operators, the strategies that would best help them access the quality of the data received by the WSN while, in the case of the IPS, these strategies would also help the network operators apply the recovery pattern that would best benefit them by keeping the cost of recovery to an optimal level. The optimality of the suggested strategies was validated both in a cluster-based deployment using SensomaX and in an IPv6-based deployment using Cooja. Future extension of this work can include the introduction of forecasting. What that basically means is that we can the iterated version of the proposed model for many different numbers of rounds, identifying each time the optimal payoff. Then, having many pairs in the form of (number of rounds, optimal payoff) it will be possible to estimate new optimal payoffs for new numbers of rounds. Furthermore, the models' applicability on networks with different densities and its scalability while network's size increases, can be further examined.

The next security-oriented work that was presented, was about a novel approach that combined VSM and Game Theory towards cyber security risk management in CI-ICSs. In particular, we created a method that takes into account the proprietary and interconnected nature of CI-ICSs and provides optimal, cost-efficient defence strategies

for the defender. This method models the cyber components of the CI-ICS as agents so that the criticality of an asset of the system can be quantified based on its interconnections to the system's components. The use case was solved as a game, with an attacker and a defender, both with their attacking and defending strategies, respectively, and as a result the Nash Equilibria, consisting of both players' optimal strategies were found. In other words, we managed to find the strategies that best serve the defender's interests and demonstrate that the game indeed has a state which no player would unilaterally want to leave from, once reaching it. Thus, we managed to show that the combination of VSM and Game Theory provides a very useful tool with excellent insight in such kind of problems. In future, this model can be further enhanced in order to cover a wider range of attack and defence strategies while validation using real data should be also considered.

In a similar fashion, VSM and Game Theory were again combined for the next presented work, in order for an ICS to be modelled and the whole setting to be treated as a two-player, zero-sum game. The viability of this CI-ICS was defined through a system of weighted components connected through weighted links, where the weights in both cases represent their importance. Once more, the defender's objective was to minimise the impact of a possible cyber attack while keeping the security costs as low as possible. That was, again, achieved by finding the Nash Equilibria of the game. This approach can be used to design defence strategies against unknown attacks, with reference only to the system's architecture.

Moving on to the next presented project, there is the Monte Carlo predictive modelling approach. Using a conceptual enterprise as a case study and verifiable historical cost of security breaches as parametric values, our model shows why using conventional risk assessment approach as budgeting process can result in significant over/under allocation of resources for cyber capabilities. To solve that, we use Monte Carlo simulation which allows us to understand the outcome of scenarios and help to understand unexpected pattern or behaviour without necessarily exposing information assets to real threats. Simulation's output is a range of values and risk assessor can derive confidence level from that range. This model can serve as a benchmark for policy and decision support to aid stakeholders in optimizing resource allocation for cyber security investments. As further work, we could include multiple resource allocation patterns for different assets, according to their role and importance within the system.

The last presented case study from the research focus on security and risk management combines Game Theory and Epidemiology in order to describe a problem where a random scanning worm (attacker) attempts to proliferate within a corporate network of 10,000 susceptible hosts and a defender attempts to mitigate that while at the same time trying to keep the security cost as low as possible. The epidemiological model is a custom one created for the needs of this research and combines SIR and SIS. The results of this use case is the recommendation to the defender of his optimal strategy which will award him with the optimal balance between network damage (by the aforementioned worm) and security cost. As shown, this strategy is not the one that would lead to the strictest possible security which is reasonable when taking into account the high cost that this would incur. Future work could very well include the adoption of a minimum security level by the defender or even the use of a topology-oriented malware that would spread more efficiently within the network. All in all, the combination of Game Theory and Epidemiology has led to a model that can provide automated recommendations to the defender on how to protect a network in a cost-efficient manner.

5.1.2 Resilience and Optimisation

As far as the resilience and optimisation oriented research is concerned, there are two different areas of focus. Firstly, a multi-beneficial application of a model that combines Game Theory and SensomaX in order to optimise non-security-related aspects of a WSN and secondly, an application of intelligent Hot-Desking, utilising real data and applied on an industrial work environment.

Beginning with the former, we managed to combine auction-based techniques and SensomaX in order to improve energy consumption, processing time and packet loss within a WSN with only a small, in most cases, impact on latency. We showed that our model can successfully improve all these aspects of the examined network compared to the case where our model does not apply. Although the proposed model demonstrated a great insight in this category of applications, it would be interesting to apply similar techniques on WSNs with specific topologies or much different densities. However, this is suggested as a scenario for future work.

Finally, we have the intelligent Hot-Desking model. In the corresponding section we managed to demonstrate a novel approach on using real occupancy data in order to provide automatic allocation of employees to free desks in a way that their productivity is maximised. We also managed to prove that this approach is not only better that the traditional, less intelligent, approaches but that it is also almost as good as an ideal (but practically impossible to be applied on a real case scenario) approach. The model is built in such a way that there are plenty of modifications that can be easily made and therefore it can be applied in numerous occasions and work environments providing a tool of great insight in its category. Thus, further work could include input from other sources apart from occupancy data, like for example personal preferences, calendar data or forecasting outputs about employees' schedules, social media data and much more.

5.2 Addressing the Research Questions

The research questions that were mentioned in section 1.4 are also mentioned here, along with a small summary of their answers and where these can be found in the thesis.

As explained in section 1.2, the answers to the research questions will be split among the three categories that were mentioned in that section (i.e. i) Critical Infrastructures and Industrial Control Systems (CI-ICSs), ii) Wireless Sensor Networks (WSNs) and iii) Hot-Desking systems). In other words each question will be addressed within the context firstly of CI-ICSs, secondly of WSNs and thirdly of Hot-Desking systems.

RQ1: Up to what level can the existing approaches improve the security and the resilience of Cyber-Physical Systems?

From the perspective of **CI-ICSs,** this research question is addressed in the second part of the sections 2.3.1.1, 2.3.1.2 and 2.3.1.4 where the omissions of the existing literature are discussed.

From the perspective of **WSNs**, this research question is addressed in the second part of the section 2.3.1.3 where the omissions of existing literature are discussed.

From the perspective of **Hot-Desking**, this research question is addressed in the second part of section 2.3.2.2 where the omissions of existing literature are discussed.

RQ2: How can we improve the security of Cyber-Physical Systems?

From the perspective of **CI-ICSs**, this research question is addressed in sections 3.3.1.1, 3.3.1.2, 3.3.2 and 3.3.3.2.The first one is about our model that combines VSM and Game Theory in order to provide cost-efficient defence solutions for CI-ICSs. The next one presents a novel approach that combines VSM with Game Theory in order to develop a risk management process which provides a holistic, cost-efficient cyber-security solution that takes into account interdependencies of critical components as well as the potential impact of different attack strategies. Section 3.3.2 expands on our Monte Carlo predicting modelling which can serve as a benchmark for policy and decision support to aid stakeholders in optimizing resource allocation for cyber security investments. Finally, the last one refers to a custom Epidemiology model that provides a cost-benefit risk management framework for managing malware spread in computer networks.

From the perspective of **WSNs**, this research question is addressed in section 3.2.2 by demonstrating how Game Theory can be used in order to build an IDS and an IPS that are applied on a WSN in order to enhance its security.

Hot-Desking systems do not participate in this research question as we do not examine a related security perspective in this work.

RQ3: How can we improve the resilience of Cyber-Physical Systems?

From the perspective of **WSNs**, this research question is addressed in section 4.2.2 by demonstrating how utilising auction-based techniques along with SensomaX, can improve energy consumption, agent processing time and packet loss in WSNs with an increase in latency that is considered trivial in most cases.

From the perspective of **Hot-Desking**, this research question is addressed in section 4.3.2. In summary, we offer a model that based on the occupancy data of the employees, calculates and suggests in real time which desk to be assigned to every

employee at the time they arrive at the organisation. The model decides which desk will make the incoming employee (or all the employees) as productive as possible, based on the project that they are working on, at that period of time. That way, not only employees find themselves working in the most productive environment possible, without having to decide the sitting arrangements themselves (with any disadvantages that this would entail in terms of the relationships among them) but also the organisation will have a double benefit as it will make profit not only due to the number of desks that will not need to be used anymore (desks will be less than the employees while still covering their needs), but also due to the fact that all employees will work under optimal productivity conditions. This is a way to improve existing Hot-Desking applications.

CI-ICSs do not participate in this research question as we do not examine a related resilience perspective in this work.

5.2.1 Final Remarks

The research presented in this thesis applies novel modelling and simulation techniques in order to improve the security and resilience of cyber-physical systems.

As far as the security perspective is concerned, we developed an IDS and an IPS, both of which are based on game-theoretic principles and are able to handle multi-dimensional strategy sets and high levels of complexity. We applied them on a WSN in order to improve its security and as a result we were able to provide the network operators with an automated mechanism that can identify the strategies that would optimally defend the WSN against an attack.

Still within the context of security, we proposed three different approaches for three use cases. Two of them combined VSM and Game Theory towards cyber security risk management in CI-ICSs. In particular, these methods take into account the proprietary and interconnected nature of a CI-ICSs in order to provide optimal, cost-efficient defence strategies for the defender. The third one used Monte Carlo predictive modelling in order to improve resource allocation for cyber security investments.

The last security-oriented use case is a unified malware proliferation model that combines the benefits of SIR and SIS along with Game Theory in order to provide a cost-benefit solution that restrains a random-scanning worm, as much as possible.

In terms of resilience-oriented research, we propose a combination of auction-based techniques and SensomaX in order to propose a light (in terms of latency surcharge) approach on reducing energy consumption, packet loss and processing time.

Finally, we present a Hot-Desking model that can be implemented in a business environment and decide the seating positions of the employees, at the time of their arrival, in a way that will maximise their total productivity.

All in all, our models manage to tackle the issues identified in existing approaches while addressing the stated research questions and ultimately, deploy a new way of Systems Thinking.

BIBLIOGRAPHY

[1] S. Beer, "Brain of the Firm: The managerial Cybernetics of organizations," *Aufl., J. Wiley&Sons, Chichester*, 1981.

[2] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *System Sciences (HICSS), 2010 43rd Hawaii International Conference on*, 2010, pp. 1–10.

[3] M. Tambe and B. An, "Game Theory for Security: A Real-World Challenge Problem for Multiagent Systems and Beyond.," in *AAAI Spring Symposium: Game Theory for Security, Sustainability, and Health*, 2012.

[4] R. B. Myerson, *Game theory*. Harvard university press, 2013.

[5] T. Spyridopoulos, G. Oikonomou, T. Tryfonas, and M. Ge, "Game theoretic approach for cost-benefit analysis of malware proliferation prevention," in *IFIP International Information Security Conference*, 2013, pp. 28–41.

[6] P. R. Thie and G. E. Keough, *An introduction to linear programming and game theory*. John Wiley & Sons, 2011.

[7] J. Matusitz, "A postmodern theory of cyberterrorism: Game theory," *Inf. Secur. J. A Glob. Perspect.*, vol. 18, no. 6, pp. 273–281, 2009.

[8] C. Schmidt, *Game theory and economic analysis: a quiet revolution in economics*. Routledge, 2003.

[9] W. O. Kermack and A. G. McKendrick, "A contribution to the mathematical theory of epidemics," *Proc. R. Soc. London. Ser. A*, vol. 115, no. 772, p. 700 LP-721, Aug. 1927.

[10] W. O. Kermack and A. G. McKendrick, "Contributions to the mathematical theory of epidemics. II. —The problem of endemicity," *Proc. R. Soc. London. Ser. A*, vol. 138, no. 834, p. 55 LP-83, Oct. 1932.

[11] W. O. Kermack and A. G. McKendrick, "Contributions to the mathematical theory of epidemics. III.—Further studies of the problem of endemicity," *Proc. R. Soc. London. Ser. A*, vol. 141, no. 843, p. 94 LP-122, Jul. 1933.

[12] V. Capasso and G. Serio, "A generalization of the Kermack-McKendrick deterministic epidemic model," *Math. Biosci.*, vol. 42, no. 1–2, pp. 43–61, 1978.

[13] H. Van der Molen, “Math on malware.,” *Inf. Syst. Audit Control Assoc. J.*, vol. 3, pp. 40–47, 2011.

[14] T. R. Peltier, *Information Security Risk Analysis*, Second Edi. Taylor & Francis, 2005.

[15] B. Karabacak and I. Sogukpinar, “ISRAM: information security risk analysis method,” *Comput. Secur.*, vol. 24, no. 2, pp. 147–159, 2005.

[16] E. ISO, “IEC 27005: 2011 (EN) Information technology--Security techniques--Information security risk management Switzerland,” *ISO/IEC*, 2011.

[17] K. Stouffer, J. Falco, and K. Scarfone, “Guide to industrial control systems (ICS) security,” *NIST Spec. Publ.*, vol. 800, no. 82, p. 16, 2011.

[18] G. Giannopoulos, R. Filippini, and M. Schimmer, “Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art,” *JRC Tech. Notes*, 2012.

[19] G. Digioia, C. Foglietta, S. Panzieri, and A. Falleni, “Mixed Holistic Reductionistic Approach for Impact Assessment of Cyber Attacks,” in *European Intelligence and Security Informatics Conference*, 2012, pp. 123–130.

[20] B. Hutchinson and M. Warren, “Information Warfare: using the viable system model as a framework to attack organisations,” *Australas. J. Inf. Syst.*, vol. 9, no. 2, 2002.

[21] J. Pita, M. Tambe, C. Kiekintveld, S. Cullen, and E. Steigerwald, “GUARDS: game theoretic security allocation on a national scale,” in *The 10th International Conference on Autonomous Agents and Multiagent Systems-Volume 1*, 2011, pp. 37–44.

[22] J. Tsai, C. Kiekintveld, F. Ordonez, M. Tambe, and S. Rathi, “IRIS-a tool for strategic security allocation in transportation networks,” 2009.

[23] J. Pita *et al.*, “Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International Airport,” in *Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track*, 2008, pp. 125–132.

[24] J. Pita *et al.*, “Using game theory for Los Angeles airport security,” *AI Mag.*, vol. 30, no. 1, p. 43, 2009.

[25] M. Esmalifalak, G. Shi, Z. Han, and L. Song, “Bad Data Injection Attack and

Defense in Electricity Market Using Game Theory Study," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 160–169, 2013.

[26] D. Kahneman, "Prospect theory: An analysis of decisions under risk," *Econometrica*, vol. 47, p. 278, 1979.

[27] J. Cox Louis Anthony, "Game theory and risk analysis," *Risk Anal. An Int. J.*, vol. 29, no. 8, pp. 1062–1068, 2009.

[28] A. Biswas and S. Karunakaran, "Cybernetic modeling of Industrial Control Systems: Towards threat analysis of critical infrastructure," *arXiv Prepr. arXiv1510.01861*, 2015.

[29] R. Böhme, "Security Metrics and Security Investment Models BT - Advances in Information and Computer Security," 2010, pp. 10–24.

[30] V. N. L. Franqueira, S. H. Houmb, and M. Daneva, "Using Real Option Thinking to Improve Decision Making in Security Investment BT - On the Move to Meaningful Internet Systems: OTM 2010," 2010, pp. 619–638.

[31] A. Mizzi, "Return on Information Security Investment-The Viability Of An Anti-Spam Solution In A Wireless Environment.," *IJ Netw. Secur.*, vol. 10, no. 1, pp. 18–24, 2010.

[32] S.-L. Wang, J.-D. Chen, P. A. Stirpe, and T.-P. Hong, "Risk-neutral evaluation of information security investment on data centers," *J. Intell. Inf. Syst.*, vol. 36, no. 3, pp. 329–345, 2011.

[33] H. Cavusoglu, H. Cavusoglu, and J. Zhang, "Security patch management: Share the burden or share the damage?," *Manage. Sci.*, vol. 54, no. 4, pp. 657–670, 2008.

[34] C. D. Huang, Q. Hu, and R. S. Behara, "An economic analysis of the optimal information security investment in the case of a risk-averse firm," *Int. J. Prod. Econ.*, vol. 114, no. 2, pp. 793–804, 2008.

[35] W. Sonnenreich, J. Albanese, and B. Stout, "Return on security investment (ROSI)-a practical quantitative model," *J. Res. Pract. Inf. Technol.*, vol. 38, no. 1, p. 45, 2006.

[36] L. J. Tallau, M. Gupta, and R. Sharman, "Information security investment decisions: evaluating the Balanced Scorecard method," *Int. J. Bus. Inf. Syst.*, vol. 5, no. 1, pp. 34–57, 2009.

[37] T. Spyridopoulos, G. Karanikas, T. Tryfonas, and G. Oikonomou, “A game theoretic defence framework against DoS/DDoS cyber attacks,” *Comput. Secur.*, vol. 38, pp. 39–50, 2013.

[38] Q. Wu, S. Shiva, S. Roy, C. Ellis, and V. Datla, “On modeling and simulation of game theory-based defense mechanisms against DoS and DDoS attacks,” in *Proceedings of the 2010 spring simulation multiconference*, 2010, p. 159.

[39] M. Asadi, C. Zimmerman, and A. Agah, “A game-theoretic approach to security and power conservation in wireless sensor networks.,” *IJ Netw. Secur.*, vol. 15, no. 1, pp. 50–58, 2013.

[40] Y. B. Reddy, “A Game Theory Approach to Detect Malicious Nodes in Wireless Sensor Networks,” in *2009 Third International Conference on Sensor Technologies and Applications*, 2009, pp. 462–468.

[41] M. Kodialam and T. V Lakshman, “Detecting network intrusions via sampling: a game theoretic approach,” in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No.03CH37428)*, 2003, vol. 3, pp. 1880–1889 vol.3.

[42] T. Alpcan and T. Basar, “A game theoretic approach to decision and analysis in network intrusion detection,” in *Decision and Control, 2003. Proceedings. 42nd IEEE Conference on*, 2003, vol. 3, pp. 2595–2600.

[43] M. Mehrandish, H. Otrok, M. Debbabi, C. Assi, and P. Bhattacharya, “NIS06-3: A Game Theoretic Approach to Detect Network Intrusions: The Cooperative Intruders Scenario,” in *IEEE Globecom 2006*, pp. 1–5.

[44] B. Krishnamachari, “An introduction to wireless sensor networks,” in *Second International Conference on Intelligent Sensing and Information Processing (ICISIP), Chennai, India*, 2005.

[45] J. Omic, A. Orda, and P. Van Mieghem, “Protecting against network infections: A game theoretic perspective,” in *28th Annual Conference IEEE INFOCOM 2009, April 19-25 2009*, 2009.

[46] P. Van Mieghem, J. Omic, and R. Kooij, “Virus spread in networks,” *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 1–14, 2009.

[47] X. Li and M. R. Lyu, “A Novel Coalitional Game Model for Security Issues in Wireless Networks,” in *IEEE GLOBECOM 2008 - 2008 IEEE Global*

Telecommunications Conference, 2008, pp. 1–6.

[48] C. Esposito and C. Choi, "Signaling game based strategy for secure positioning in wireless sensor networks," *Pervasive Mob. Comput.*, vol. 40, pp. 611–627, 2017.

[49] N. Basilico, N. Gatti, M. Monga, and S. Sicari, "Security Games for Node Localization through Verifiable Multilateration," *IEEE Trans. Dependable Secur. Comput.*, vol. 11, no. 1, pp. 72–85, 2014.

[50] J. Wu, K. Ota, M. Dong, and C. Li, "A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities.," *IEEE Access*, vol. 4, no. 4, pp. 416–424, 2016.

[51] A. Attiah, M. Chatterjee, and C. C. Zou, "A Game Theoretic Approach to Model Cyber Attack and Defense Strategies," in *2018 IEEE International Conference on Communications (ICC)*, 2018, pp. 1–7.

[52] S. A. Zonouz, H. Khurana, W. H. Sanders, and T. M. Yardley, "RRE: A Game-Theoretic Intrusion Response and Recovery Engine," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 395–406, 2014.

[53] H. Andersson and T. Britton, "Stochastic epidemic models and their statistical analysis," 2000.

[54] Y. Wang, S. Wen, Y. Xiang, and W. Zhou, "Modeling the propagation of worms in networks: A survey," *IEEE Commun. Surv. Tutorials*, vol. 16, no. 2, pp. 942–960, 2014.

[55] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Phys. Rev. Lett.*, vol. 86, no. 14, p. 3200, 2001.

[56] J. Kim, S. Radhakrishnan, and S. K. Dhall, "Measurement and analysis of worm propagation on Internet network topology," in *Proceedings. 13th International Conference on Computer Communications and Networks (IEEE Cat. No.04EX969)*, 2004, pp. 495–500.

[57] B. K. Mishra and S. K. Pandey, "Dynamic model of worm propagation in computer network," *Appl. Math. Model.*, vol. 38, no. 7–8, pp. 2173–2179, 2014.

[58] Z. Chen and C. Ji, "Spatial-temporal modeling of malware propagation in networks," *IEEE Trans. Neural Networks*, vol. 16, no. 5, pp. 1291–1303, 2005.

[59] C. C. Zou, W. Gong, and D. Towsley, "Code red worm propagation modeling

and analysis," in *Proceedings of the 9th ACM conference on Computer and communications security*, 2002, pp. 138–147.

[60] S. Shen *et al.*, "A non-cooperative non-zero-sum game-based dependability assessment of heterogeneous WSNs with malware diffusion," *J. Netw. Comput. Appl.*, vol. 91, pp. 26–35, 2017.

[61] S. Shen, H. Li, R. Han, A. V Vasilakos, Y. Wang, and Q. Cao, "Differential Game-Based Strategies for Preventing Malware Propagation in Wireless Sensor Networks," *IEEE Trans. Inf. Forensics Secur.*, vol. 9, no. 11, pp. 1962–1973, 2014.

[62] H.-Y. Shi, W.-L. Wang, N.-M. Kwok, and S.-Y. Chen, "Game Theory for Wireless Sensor Networks: A Survey," *Sensors*, vol. 12, no. 7. pp. 9055–9097, 2012.

[63] H. Ren and M. Q.-. Meng, "Game-Theoretic Modeling of Joint Topology Control and Power Scheduling for Wireless Heterogeneous Sensor Networks," *IEEE Trans. Autom. Sci. Eng.*, vol. 6, no. 4, pp. 610–625, 2009.

[64] M. Ayers and Y. Liang, "Gureen Game: An energy-efficient QoS control scheme for wireless sensor networks," in *2011 International Green Computing Conference and Workshops*, 2011, pp. 1–8.

[65] M. L. Tsetlin, *Automaton theory and modeling of biological systems, volume 102 of Mathemat ics in Science and Engineering*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1973.

[66] D. Xie, Q. Sun, Q. Zhou, Y. Qiu, and X. Yuan, "An Efficient Clustering Protocol for Wireless Sensor Networks Based on Localized Game Theoretical Approach," *Int. J. Distrib. Sens. Networks*, vol. 9, no. 8, p. 476313, Aug. 2013.

[67] G. Koltsidas and F.-N. Pavlidou, "A game theoretical approach to clustering of ad-hoc and sensor networks," *Telecommun. Syst.*, vol. 47, no. 1, pp. 81–93, 2011.

[68] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," in *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*, 2000, p. 10 pp. vol.2.

[69] S. Sengupta, M. Chatterjee, and K. Kwiat, "A Game Theoretic Framework for Power Control in Wireless Sensor Networks," *IEEE Trans. Comput.*, vol. 59, no.

2, pp. 231–242, 2010.

[70] E. Campos-Nañez, A. Garcia, and C. Li, “A game-theoretic approach to efficient power management in sensor networks,” *Oper. Res.*, vol. 56, no. 3, pp. 552–561, 2008.

[71] M. Esmaeeli and S. A. H. Ghahroudi, “Improving energy efficiency using a new game theory algorithm for wireless sensor networks,” *Int. J. Comput. Appl.*, vol. 136, no. 12, 2016.

[72] P. Kuila and P. K. Jana, “Energy efficient load-balanced clustering algorithm for wireless sensor networks,” *Procedia Technol.*, vol. 6, pp. 771–777, 2012.

[73] G. Gupta and M. F. Younis, “Load-balanced clustering of wireless sensor networks.,” in *ICC*, 2003, vol. 3, pp. 1848–1852.

[74] J. Duan, D. Gao, D. Yang, C. H. Foh, and H. Chen, “An Energy-Aware Trust Derivation Scheme With Game Theoretic Approach in Wireless Sensor Networks for IoT Applications,” *IEEE Internet Things J.*, vol. 1, no. 1, pp. 58–69, 2014.

[75] M. A. Abd, S. F. M. A. Rubeaai, K. E. Tepe, and R. Benlamri, “Game theoretic energy balancing routing in three dimensional wireless sensor networks.,” in *WCNC*, 2015, pp. 1596–1601.

[76] A. Hirst, “Settlers, vagrants and mutual indifference: unintended consequences of hot-desking,” *J. Organ. Chang. Manag.*, vol. 24, no. 6, pp. 767–788, Oct. 2011.

[77] S. Halford, “‘Towards a Sociology of Organizational Space,’” *Sociol. Res. Online*, vol. 9, no. 1, pp. 1–16, Feb. 2004.

[78] L. J. Millward, S. A. Haslam, and T. Postmes, “Putting employees in their place: The impact of hot desking on organizational and team identification,” *Organ. Sci.*, vol. 18, no. 4, pp. 547–559, 2007.

[79] A. Felstead, N. Jewson, and S. Walters, *Changing places of work*. Palgrave Macmillan, 2005.

[80] A. Leaman and B. Bordass, “Productivity in buildings: the ‘killer’ variables,” *Build. Res. Inf.*, vol. 27, no. 1, pp. 4–19, Jan. 1999.

[81] D. Clements-Croome, “Indoor environment and productivity,” in *Creating the productive workplace*, Taylor & Francis, 2006, pp. 53–82.

[82] B. P. Haynes, “Office productivity: a theoretical framework,” *J. Corp. Real Estate*, vol. 9, no. 2, pp. 97–110, 2007.

[83] J. Sydow, L. Lindkvist, and R. DeFillippi, “Project-based organizations, embeddedness and repositories of knowledge,” *Organ. Stud.*, vol. 25, no. 9, pp. 1475–1489, 2004.

[84] P. Leather, D. Beale, and L. Sullivan, “Noise, psychosocial stress and their interaction in the workplace,” *J. Environ. Psychol.*, vol. 23, no. 2, pp. 213–222, 2003.

[85] J. Kim and R. de Dear, “Nonlinear relationships between individual IEQ factors and overall workspace satisfaction,” *Build. Environ.*, vol. 49, pp. 33–40, 2012.

[86] J. H. Yamamura and J. W. Westerman, “Generational preferences for work environment fit: effects on employee outcomes,” *Career Dev. Int.*, vol. 12, no. 2, pp. 150–161, Apr. 2007.

[87] B. C. O. CABE, “The impact of office design on business performance, Commission for Architecture and the Built Environment,” *Br. Counc. Off.*, 2005.

[88] D. P. Wyon, “The effects of indoor air quality on performance and productivity,” *Indoor Air*, vol. 14, no. 7, pp. 92–101, 2004.

[89] World Green Building Society, “Health, Wellbeing & Productivity in Offices,” 2014.

[90] Public Health England, “The impact of physical environments on employee wellbeing-topic overview,” 2015.

[91] A. Felstead, “Rapid change or slow evolution? Changing places of work and their consequences in the UK,” *J. Transp. Geogr.*, vol. 21, pp. 31–38, 2012.

[92] K. Mirchandani, “‘The Best of Both Worlds’ and ‘Cutting My Own Throat’: Contradictory Images of Home-Based Work,” *Qual. Sociol.*, vol. 23, no. 2, pp. 159–182, 2000.

[93] N. D. Gilson, A. Suppini, G. C. Ryde, H. E. Brown, and W. J. Brown, “Does the use of standing ‘hot’desks change sedentary work time in an open plan office?,” *Prev. Med. (Baltim).*, vol. 54, no. 1, pp. 65–67, 2012.

[94] J. Y. Chau *et al.*, “The effectiveness of sit-stand workstations for changing office workers’ sitting time: results from the Stand@Work randomized controlled trial pilot,” *Int. J. Behav. Nutr. Phys. Act.*, vol. 11, no. 1, p. 127, 2014.

[95] J. Y. Chau *et al.*, “Are workplace interventions to reduce sitting effective? A systematic review,” *Prev. Med. (Baltim).*, vol. 51, no. 5, pp. 352–356, 2010.

[96] L. Straker, R. A. Abbott, M. Heiden, S. E. Mathiassen, and A. Toomingas, “Sit–stand desks in call centres: Associations of use and ergonomics awareness with sedentary behavior,” *Appl. Ergon.*, vol. 44, no. 4, pp. 517–522, 2013.

[97] T. A. Alkhajah, M. M. Reeves, E. G. Eakin, E. A. H. Winkler, N. Owen, and G. N. Healy, “Sit–stand workstations: a pilot intervention to reduce office sitting time,” *Am. J. Prev. Med.*, vol. 43, no. 3, pp. 298–303, 2012.

[98] J. Y. Chau, M. Daley, A. Srinivasan, S. Dunn, A. E. Bauman, and H. P. van der Ploeg, “Desk-based workers’ perspectives on using sit-stand workstations: a qualitative analysis of the Stand@Work study,” *BMC Public Health*, vol. 14, no. 1, p. 752, 2014.

[99] ISA SP99, “Security for Industrial Automation and Control Systems.” Part 1-1.

[100] P. Ilia, G. Oikonomou, and T. Tryfonas, “Cryptographic Key Exchange in IPv6-Based Low Power, Lossy Networks,” in *Information Security Theory and Practice. Security of Mobile and Cyber-Physical Systems*, 2013, pp. 34–49.

[101] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, “Wireless sensor network security: A survey,” *Secur. Distrib. grid, mobile, pervasive Comput.*, vol. 1, p. 367, 2007.

[102] W. Dargie and C. Poellabauer, *Fundamentals of wireless sensor networks: theory and practice*. John Wiley & Sons, 2010.

[103] K. Sohraby, D. Minoli, and T. Znati, *Wireless sensor networks: technology, protocols, and applications*. John Wiley & Sons, 2007.

[104] I. Lambrou, “IPv6 Security in the Internet of Things,” University of Bristol, 2012.

[105] D. Puccinelli and M. Haenggi, “Wireless sensor networks: applications and challenges of ubiquitous sensing,” *IEEE Circuits Syst. Mag.*, vol. 5, no. 3, pp. 19–31, 2005.

[106] R. Weeks, “Wireless sensor test bed to provide guidelines for industrial systems.” [Online]. Available: https://inlportal.inl.gov/portal/server.pt?open=514&objID=1269&mode=2&featurestory=DA_5350%0A20.

[107] D. E. R. Denning, *Information warfare and security*, vol. 4. Addison-Wesley Reading, MA, 1999.

[108] F. L. Lewis, “Wireless sensor networks,” *Smart Environ. Technol. Protoc. Appl.*, pp. 11–46, 2004.

[109] P. S. K. Jena, “Security in Wireless Sensor Networks.” .

[110] K. Sharma and M. K. Ghose, “Wireless sensor networks: An overview on its security threats,” *IJCA, Spec. Issue “Mobile Ad-hoc Networks” MANETs*, pp. 42–45, 2010.

[111] N. A. Alrajeh, S. Khan, and B. Shams, “Intrusion detection systems in wireless sensor networks: a review,” *Int. J. Distrib. Sens. Networks*, vol. 9, no. 5, p. 167575, 2013.

[112] H. Jadidoleslamy, “Designing an Agent-Based Intrusion Detection System for Heterogeneous Wireless Sensor Networks: Robust, Fault Tolerant and Dynamic Reconfigurable,” *Int. J. Commun. Netw. Syst. Sci.*, vol. 4, no. 08, p. 523, 2011.

[113] K. Scarfone and P. Mell, “Guide to intrusion detection and prevention systems (idps),” *NIST Spec. Publ.*, vol. 800, no. 2007, p. 94, 2007.

[114] M. S. I. Mamun and A. F. M. Kabir, “Hierarchical design based intrusion detection system for wireless ad hoc network,” *arXiv Prepr. arXiv1208.3772*, 2012.

[115] M. E. Whitman and H. J. Mattord, “Principles of Information Security. Cengage Learning EMEA,” ISBN 978-1-4239-0177-8. Google Scholar, 2009.

[116] S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari, “Challenges in applying game theory to the domain of information warfare,” in *Information Survivability Workshop (ISW)*, 2002.

[117] S. N. Hamilton, W. L. Miller, A. Ott, and O. S. Saydjari, “The role of game theory in information warfare,” in *4th Information survivability workshop (ISW-2001/2002)*, 2002.

[118] B. Chandrasekaran, “Survey of network traffic models,” *Waschingt. Univ. St. Louis CSE*, vol. 567, 2009.

[119] H. S. Bedi, S. Roy, and S. Shiva, “Game theory-based defense mechanisms against DDoS attacks on TCP/TCP-friendly flows,” in *Computational Intelligence in Cyber Security (CICS), 2011 IEEE Symposium on*, 2011, pp. 129–136.

[120] G. Vining and S. Kowalski, *Statistical Methods for Engineers, 3rd Edition*. 2011.

[121] M. Haghighi and D. Cliff, “Sensomax: An agent-based middleware for decentralized dynamic data-gathering in wireless sensor networks,” in *2013 International Conference on Collaboration Technologies and Systems (CTS)*, 2013, pp. 107–114.

[122] M. Haghighi and D. Cliff, “Multi-agent Support for Multiple Concurrent Applications and Dynamic Data-Gathering in Wireless Sensor Networks,” in *2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, 2013, pp. 320–325.

[123] M. Haghighi, “An agent-based multi-model tool for simulating multiple concurrent applications in WSNs,” in *Journal of Advances in Computer Networks (JACN), 5th International Conference on Communication Software and Networks*, 2013.

[124] F. Österlind, “A sensor network simulator for the Contiki OS,” *SICS Res. Rep.*, 2006.

[125] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, “Transmission of IPv6 packets over IEEE 802.15. 4 networks,” 2007.

[126] T. Winter *et al.*, “RPL: IPv6 routing protocol for low-power and lossy networks,” 2012.

[127] S. Klipper, *Information Security Risk Management*. Wiesbaden: Springer Fachmedien Wiesbaden, 2015.

[128] G. Stoneburner, A. Goguen, and A. Feringa, “Risk management guide for information technology systems,” Gaithersburg, MD, 2002.

[129] L. Rajbhandari and E. A. Snekkenes, “Mapping between Classical Risk Management and Game Theoretical Approaches,” in *Communications and Multimedia Security*, 2011, pp. 147–154.

[130] M. Cheminod *et al.*, “Detecting Chains of Vulnerabilities in Industrial Networks,” *IEEE Trans. Ind. Informatics*, vol. 5, no. 2, pp. 181–193, May 2009.

[131] H. Kjell, “Probabilistic Risk Analysis and Game Theory,” *Risk Anal.*, vol. 22, no. 1, pp. 17–27, 2002.

[132] G. Levitin, “Optimal Defense Strategy Against Intentional Attacks,” *IEEE Trans. Reliab.*, vol. 56, no. 1, pp. 148–157, Mar. 2007.

[133] S. Beer, “The Viable System Model: Its Provenance, Development, Methodology

and Pathology," *J. Oper. Res. Soc.*, vol. 35, no. 1, pp. 7–25, Jan. 1984.

[134] G. Levitin and K. Hausken, "Redundancy vs. protection vs. false targets for systems under attack," *IEEE Trans. Reliab.*, vol. 58, no. 1, pp. 58–68, 2009.

[135] T. Spyridopoulos, K. Maraslis, T. Tryfonas, G. Oikonomou, and S. Li, "Managing cyber security risks in industrial control systems with game theory and viable system modelling," in *2014 9th International Conference on System of Systems Engineering (SOSE)*, 2014, pp. 266–271.

[136] P. J. Steinbart, R. L. Raschke, G. Gal, and W. N. Dilla, "SECURQUAL: An instrument for evaluating the effectiveness of enterprise information security programs," *J. Inf. Syst.*, vol. 30, no. 1, pp. 71–92, 2015.

[137] L. Demetz and D. Bachlechner, "To invest or not to invest? Assessing the economic viability of a policy and security configuration management tool," in *The Economics of Information Security and Privacy*, Springer, 2013, pp. 25–47.

[138] D. Chinn, J. Kaplan, and A. Weinberg, "Risk and responsibility in a hyperconnected world: Implications for enterprises," *A Rep. from McKinsey Co.*, 2014.

[139] D. W. Straub and R. J. Welke, "Coping with systems risk: security planning models for management decision making," *MIS Q.*, pp. 441–469, 1998.

[140] B. Srinidhi, J. Yan, and G. K. Tayi, "Allocation of resources to cyber-security: The effect of misalignment of interest between managers and investors," *Decis. Support Syst.*, vol. 75, pp. 49–62, 2015.

[141] Lee Bell et al., "TalkTalk hack: ICO fines TalkTalk a record £400,000 for data breach." [Online]. Available: http://www.itpro.co.uk/security/24136/talktalk-hack-icofines- talktalk-a-record-400000-for-data-breach. [Accessed: 23-Sep-2016].

[142] G. Cluley, "Six months on from the TalkTalk hack - how has the firm suffered?," 2016. [Online]. Available: https://www.grahamcluley.com/talktalk-hack/. [Accessed: 23-Sep-2016].

[143] E. Burtescu, "Decision assistance in risk assessment-monte carlo simulations," *Inform. Econ.*, vol. 16, no. 4, p. 86, 2012.

[144] V. Molak and V. (ed. . Molak, *Fundamentals of risk analysis and risk management*. Boca Raton: Lewis Publishers, 1997.

[145] A. Calder and S. G. Watkins, *Information security risk management for ISO27001/ISO27002*. It Governance Ltd, 2010.

[146] United States. General Accounting Office, "Information Security Risk Assessment Practices of Leading Organizations: A Supplement to GAO's May 1998 Executive Guide on Information Security Management," 1999.

[147] Enisa, "Introduction to Return on Security Investment," 2015.

[148] T. Fagade and T. Tryfonas, "Security by Compliance? A Study of Insider Threat Implications for Nigerian Banks," in *Human Aspects of Information Security, Privacy, and Trust*, 2016, pp. 128–139.

[149] L. A. Gordon and M. P. Loeb, "Budgeting Process for Information Security Expenditures," *Commun. ACM*, vol. 49, no. 1, pp. 121–125, Jan. 2006.

[150] F. Massacci, R. Ruprai, M. Collinson, and J. Williams, "Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers," *IEEE Secur. Priv.*, vol. 14, no. 3, pp. 52–60, 2016.

[151] R. Rue, S. L. Pfleeger, and D. Ortiz, "A Framework for Classifying and Comparing Models of Cyber Security Investment to Support Policy and Decision-Making.," in *WEIS*, 2007.

[152] RiskAMP, "Risk Analysis Using Monte Carlo Simulation," 2016.

[153] Ponemon Institute, "Cost of Data Breach," 2015.

[154] Kaspersky Lab, "Damage Control: The Cost of Security Breaches," 2015.

[155] D. Lyon, "Modeling Security Investments With Monte Carlo Simulations," 2014.

[156] M. Van Hauwermeiren and D. Vose, *A Compendium of Distributions*. 2009.

[157] J. Turim, "Should We Risk It? David M. Kammen and David M. Hassenzahl, Princeton University Press, Princeton, New Jersey, 1999," *Risk Anal.*, vol. 19, no. 5, p. 1017, 1999.

[158] M. Van Dijk, A. Juels, A. Oprea, and R. L. Rivest, "FlipIt: The game of 'stealthy takeover,'" *J. Cryptol.*, vol. 26, no. 4, pp. 655–713, 2013.

[159] M. M. Saudi, E. M. Tamil, A. J. Cullen, M. E. Woodward, and M. Y. I. Idris, "Reverse engineering: EDOWA worm analysis and classification," in *Advances in Electrical Engineering and Computational Science*, Springer, 2009, pp. 277–288.

[160] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver,

"Inside the slammer worm," *IEEE Secur. Priv.*, vol. 99, no. 4, pp. 33–39, 2003.

[161] S. Staniford, V. Paxson, and N. Weaver, "How to Own the Internet in Your Spare Time.," in *USENIX security symposium*, 2002, vol. 2, pp. 14–15.

[162] M. Vojnovic and A. J. Ganesh, "On the race of worms, alerts, and patches," *IEEE/ACM Trans. Netw.*, vol. 16, no. 5, pp. 1066–1079, 2008.

[163] D. Moore and C. Shannon, "Code-Red: a case study on the spread and victims of an Internet worm," in *Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurment*, 2002, pp. 273–284.

[164] C. Shannon and D. Moore, "The spread of the witty worm," *IEEE Secur. Priv.*, vol. 2, no. 4, pp. 46–50, 2004.

[165] C. E. Lemke and J. Howson Joseph T, "Equilibrium points of bimatrix games," *J. Soc. Ind. Appl. Math.*, vol. 12, no. 2, pp. 413–423, 1964.

[166] L. S. Shapley, "A note on the Lemke-Howson algorithm," in *Pivoting and Extension*, Springer, 1974, pp. 175–189.

[167] B. Von Stengel, "Computing equilibria for two-person games," *Handb. game theory with Econ. Appl.*, vol. 3, pp. 1723–1759, 2002.

[168] M. Haghighi, "Market-Based Resource Allocation for Energy-Efficient Execution of Multiple Concurrent Applications in Wireless Sensor Networks BT - Mobile, Ubiquitous, and Intelligent Computing," 2014, pp. 173–178.

[169] M. Haghighi, "Cooperative Task Allocation in Utility-based Clustered Wireless Sensor Networks," *Int. J. Inf. Electron. Eng.*, 2013.

[170] A. M. Townsend, *Smart Cities: Big Data, Civic Hackers, and the Quest for a New Utopia*. New York: WW Norton & Company, 2013.

[171] S. Dirks and M. Keeling, "A vision of smarter cities: How cities can lead the way into a prosperous and sustainable future," 2009.

[172] M. Webb *et al.*, "Information marketplaces: The new economics of cities," *Clim. Group, Arup, Accent. Horiz.*, 2011.

[173] E. Glaeser, *Triumph of the city : how our greatest invention makes us richer, smarter, greener, healthier, and happier*. Penguin Press, 2011.

[174] R. J. Cole, A. Bild, and A. Oliver, "The changing context of knowledge-based work: consequences for comfort, satisfaction and productivity," *Intell. Build. Int.*, vol. 4, no. 3, pp. 182–196, 2012.

[175] D. Ricci, “Big Data Management,” 2014.

[176] C. Jones and A. Orr, “Spatial Economic Change and Long-term Urban Office Rental Trends,” *Reg. Stud.*, vol. 38, no. 3, pp. 281–292, 2004.

[177] D. Harris, “Turning office desks into hot property,” *The Sunday Times,(ed.)*, 1992.

[178] C. Stuart, “Change in the Workplace – what motivates people at work?,” 2014.

[179] Anonymised director at major UK banking firm, “Interview on issues affecting the office work place in banking context,” 2012.

[180] Y. El Iraki, “MySeat Occupancy Solutions,” 2015.

[181] L. Suzuki, P. Cooper, T. Tryfonas, and G. Oikonomou, “Hidden Presence: Sensing Occupancy and Extracting Value from Occupancy Data BT - Design, User Experience, and Usability: Interactive Experience Design,” 2015, pp. 412–424.